SENSIBILIZACIÓN SOBRE LA NECESIDAD DE TOMAR MEDIDAS CONTRA LAS CIBERAMENAZAS

Trabajo Fin de Máster

Autores: PEDRO MARTÍN BARROS BARRIOS

JULIÁN DAVID APONTE DÍAZ

Tutor: FERNANDO LLORENTE SANTOS

Máster en Ciberdefensa

MCD

Universidad de Alcalá

Fundación IN-NOVA Centro de Innovación

Trabajo Fin de Máster

SENSIBILIZACIÓN SOBRE LA NECESIDAD DE TOMAR MEDIDAS CONTRA LAS CIBERAMENAZAS

Autores: PEDRO MARTÍN BARROS BARRIOS
JULIÁN DAVID APONTE DÍAZ

Tutor: FERNANDO LLORENTE SANTOS

Fecha de Presentación: abril de 2018

Máster en Ciberdefensa, 2ª edición

Universidad de Alcalá

TABLA DE CONTENIDO

1. LISTADO DE FIGURAS

2. LISTADO DE ABREVIATURAS

CERT	Equipo de Respuesta a Emergencias Cibernéticas (Por sus siglas en inglés Computer Emergency Response Team)
CSIRT	Equipo de Respuesta ante Incidentes de Seguridad (Por sus siglas en inglés Computer Security Incident Response Team)
DOFA	Debilidades, Oportunidades, Fortalezas y Amenazas
GPS	Sistema de Posicionamiento Global (Por sus siglas en inglés Global Positioning System)
IP	Protocolo de Internet (Por sus siglas en inglés Internet Protocol)
IRC	Chat de Relé en Internet (Por sus siglas en inglés Internet Relay Chat)
MAC	Control de Acceso a Medios (Por sus siglas en inglés Media Access Control)
MITM	Hombre en el Medio (Por sus siglas en inglés Man In The Middle)
SQL	Lenguaje de Consulta Estructurado (Por sus siglas en inglés Structured Query Language)
TI	Tecnologías de Información
TIC	Tecnología de la Información y las Comunicaciones
USB	Bus de Serie Universal (Por sus siglas en Inglés Universal Serial Bus)

3. GLOSARIO DE TÉRMINOS

AMENAZA CIBERNÉTICA: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado [1].

ATAQUE CIBERNÉTICO: Acción Organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema a través del ciberespacio [1].

CIBERESPACIO: Es el ambiente, tanto físico como virtual, compuesto por sistemas computacionales, programas y aplicaciones (software), redes de telecomunicaciones incluido el internet, datos e información y la infraestructura física asociada que es utilizada para la interacción entre usuarios, entre máquinas y entre máquinas y usuarios [1].

CIBERNÉTICA: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio; así como el empleo de las capacidades militares ante amenazas o actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales [2].

CIBERSEGURIDAD: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio [1].

RIESGO: Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas [1].

SEGURIDAD DIGITAL: Es la situación de normalidad y de tranquilidad en el Entorno Digital / Ciberespacio, derivada de la realización de los fines esenciales del Estado y de la gestión del riesgo, que demanda la voluntad social y política de todas las múltiples partes interesadas y de los ciudadanos del país [1].

VULNERABILIDAD: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan [1].

4. INTRODUCCIÓN

4.1. EL FUERTE VÍNCULO ENTRE EL HOMBRE Y LA TECNOLOGÍA

Las Tecnologías de la Información y las comunicaciones hoy en día son una realidad en la vida del ser humano, en todos los ámbitos de la sociedad actual; en la actualidad dichas tecnologías se han hecho tan inherentes a la vida de las personas, que ya ni siquiera se ven obligadas a realizar consultas sobre el tema, todo esto debido a que el vínculo hombre – tecnología es cada vez más estrecho.

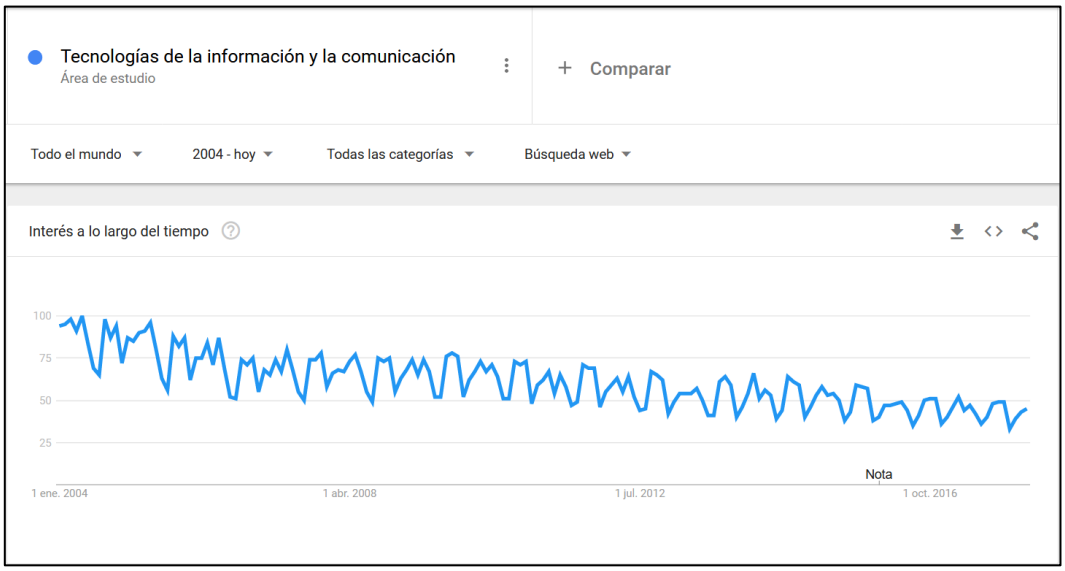

Figura 1 - Histórico de búsquedas relacionadas con TIC en Google (Fuente: Google Trends)

La Figura 1 permite evidenciar lo expuesto anteriormente; en dicha gráfica se evidencia del resultado de un sencillo análisis realizado a través de la herramienta Google Trends; en ella se muestra el histórico de las búsquedas relacionadas con el área de Tecnologías de la información y la comunicación, encontrando que para el año 2004 era una de las áreas más consultadas en Google; esto teniendo en cuenta el auge de las TIC que sufre un fuerte impulso al inicio del presente siglo; sin embargo, comparado con la tendencia de búsqueda hoy en día, se observa una disminución relevante en la tendencia.

Es importante resaltar que hoy en día existen múltiples TIC's y que todas ellas hacen uso del ciberespacio como medio de transporte de la información que se intercambia entre diferentes tipos de dispositivos; el ciberespacio es un concepto muy amplio dentro del cual una de las partes más grandes es la red conocida como Internet; dicha red no sólo es grande por el tamaño de la infraestructura que la sostiene sino por la cantidad de información que transita a través de ella, una muestra clara de ello se puede apreciar en la cantidad de eventos que se pueden generar en tan sólo un minuto.

En la siguiente figura, se muestra las enormes cantidades de información que se intercambian a través de las plataformas web más reconocidas, no obstante, en dicha imagen no se presenta información sobre otras múltiples plataformas que no son de tan grandes dimensiones; lo anterior es sólo una apreciación que le permitiría a una persona dimensionar la cantidad de datos que pueden transitar en Internet por tan sólo un minuto [3].

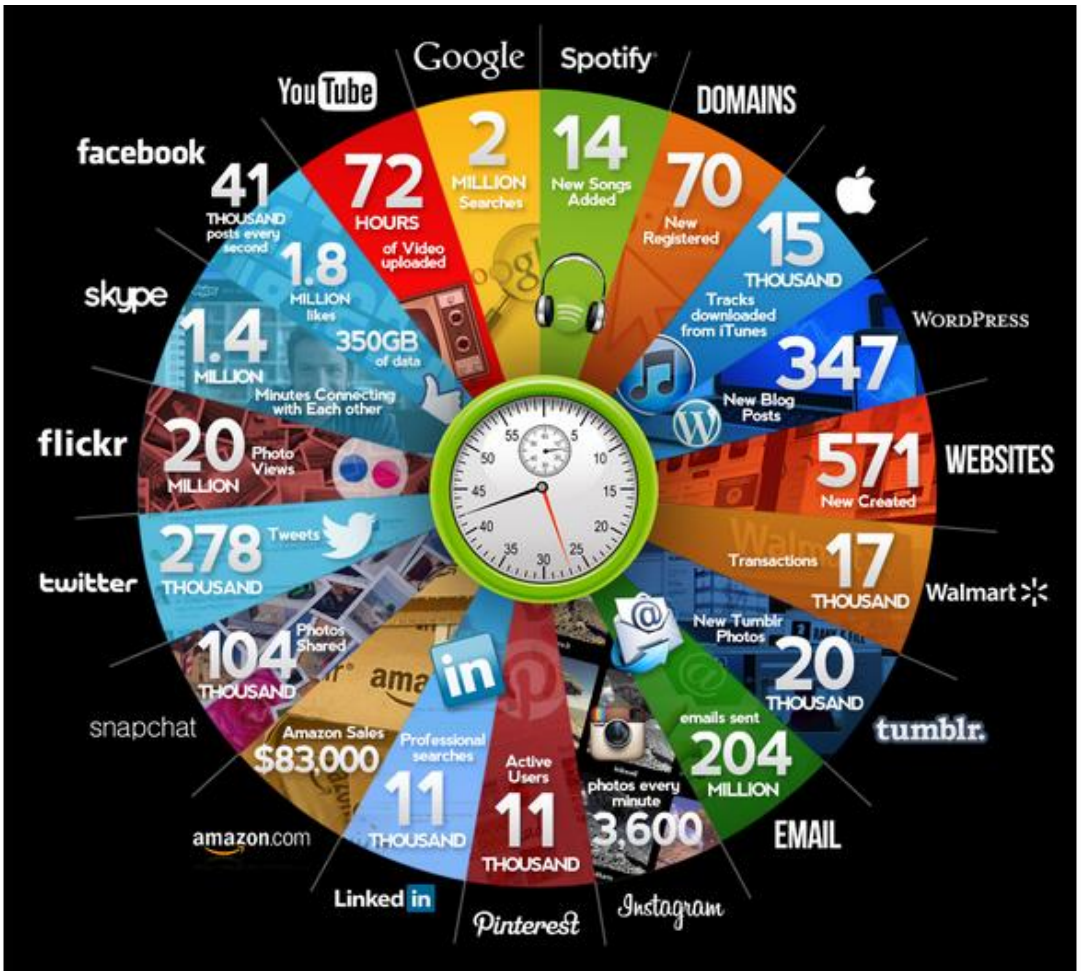

Figura 2 - Qué sucede en Internet en 60 segundos (Fuente: https://blog.qmee.com/qmee-online-in-60-seconds/)

4.2. EL CRECIMIENTO DE LA AMENAZA EN EL CIBERESPACIO

El fuerte vínculo del ser humano con las tecnologías actuales y la creciente cantidad de información que transita a través de Internet y las demás redes informáticas ha generado que las amenazas aumenten también de forma exponencial, como se aprecia en un estudio realizado por la compañía OPSWAT sobre el crecimiento, entre 1995 y el 2013, de una de las amenazas más comunes en el ciberespacio, el malware [4].

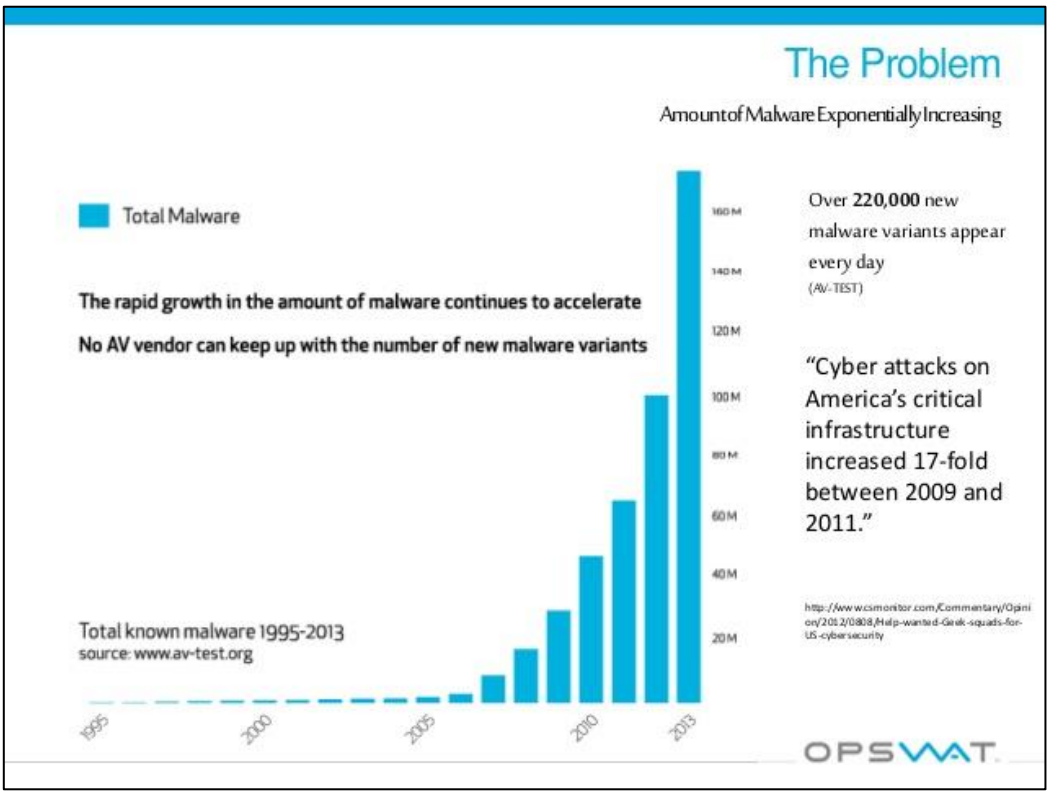

Figura 3 – Estudio sobre el crecimiento del malware entre 1995 y 2013 (Fuente: http://cybersecurity.jhigh.co.uk/images/malwareGrowth2.jpg)

Según dicho estudio, para la fecha en que se realizó el mismo; el promedio de crecimiento de malware era de 220.000 nuevas variantes de malware por día [4], una cifra muy preocupante, si se tiene en cuenta que la Internet es utilizada actualmente no sólo como medio de comunicación personal, sino que es el soporte de Infraestructuras Críticas Digitales, las cuales permiten el normal funcionamiento de los Estados a través del ciberespacio.

Frente a esta situación el ser humano ha establecido diferentes métodos de protección, enfocados principalmente en el diseño de sistemas que permitan contrarrestar los vectores de ataque adoptados por las fuentes de amenaza; sin embargo, dichos sistemas parecen no haber sido suficiente para mitigar los riesgos de forma relevante, ya que como muestra un análisis del portal Magazcitum, los incidentes informáticos hasta el 2015 se han mantenido al alza, como se muestra a continuación [5].

Figura 4 - Evolución de los incidentes informáticos, desde el 2009 hasta el 2015 (Fuente: http://www.magazcitum.com.mx/?p=3446#.WrGAf-ch2XA)

4.3. ESTRATEGIAS ACTUALES FRENTE A LAS AMENAZAS

Como se mencionó anteriormente, frente al aumento de amenazas cibernéticas y de incidentes de seguridad informática, la tendencia ha sido generar nuevas tecnologías; muestra de ello se aprecia en una noticia publicada en el portal de MVA Electrotecnia, donde se afirma que entre el 2013 y el 2019 la tendencia de los ingresos de la industria de la Ciberseguridad se mantiene en crecimiento y se prevé que para el 2019 de habrán suplicado, lo que demuestra el importante crecimiento dentro de este sector [6].

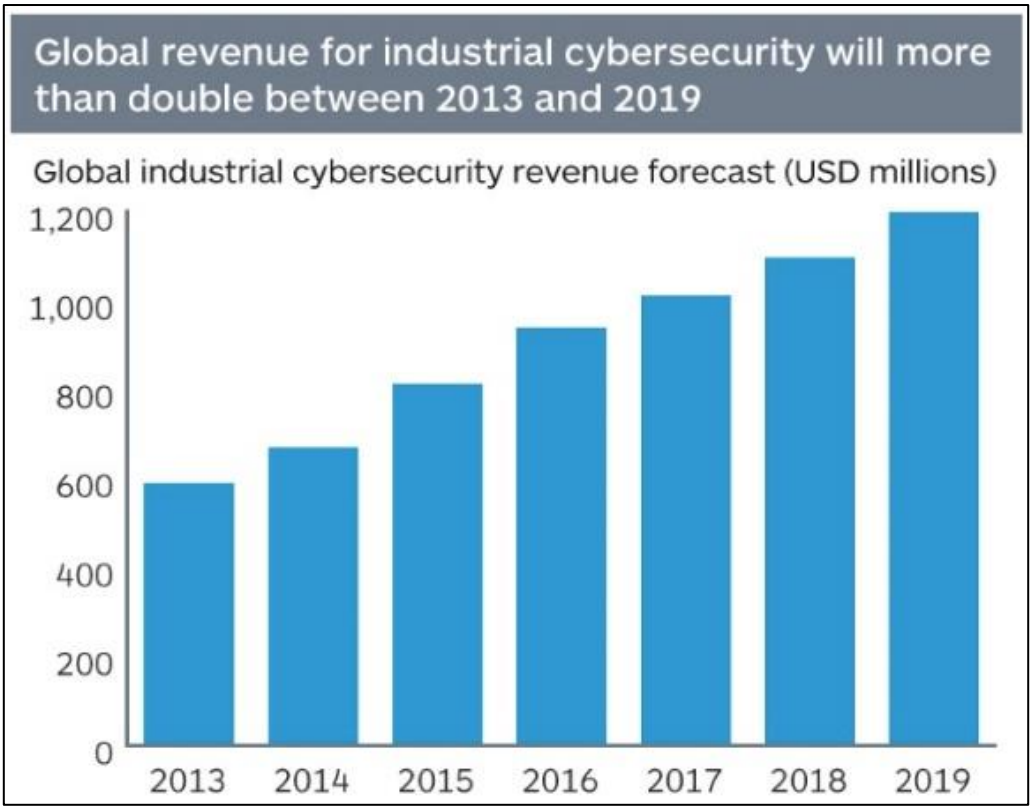

Figura 5 - Crecimiento de los ingresos dentro de la industria de la Ciberseguridad (Fuente: http://www.mva.pt/info/noticias/1239)

4.4. RESULTADOS DE LAS ESTRATEGIAS ACTUALES

Con los valores expuestos hasta el momento y realizando una proyección con base en la tendencia, se puede realizar un análisis sobre el impacto generado por la creciente industria de ciberseguridad frente al crecimiento de la amenaza y los incidentes que esta viene generando, para ello se colocarán los valores y sus respectivas proyecciones en una tabla, como se muestra a continuación.

Tabla 1 – Resumen crecimiento de la amenaza Vs. Crecimiento tecnológico (Fuente: Elaboración propia)

AÑO	CANTIDAD DE FAMILIAS DE MALWARE	CANTIDAD DE INCIDENTES	INDUSTRIA DE CIBERSEGURIDAD (MILLONES DE USD)
2009	27.000.000	3.400.000	156.666.667
2010	42.000.000	9.400.000	266.666.667
2011	61.000.000	22.700.000	376.666.667
2012	100.000.000	24.900.000	486.666.667
2013	170.000.000	29.900.000	600.000.000
2014	183.200.000	42.900.000	700.000.000
2015	217.600.000	59.200.000	820.000.000

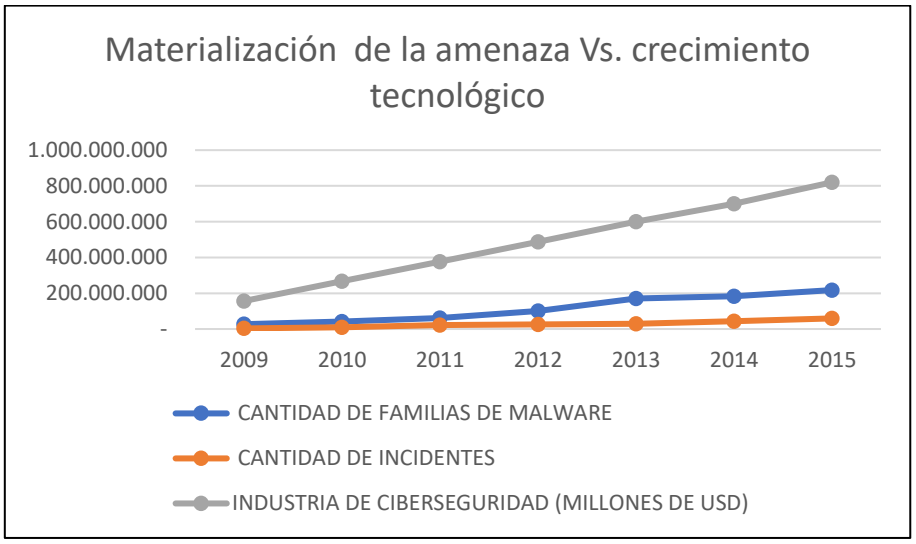

Figura 6 - Materialización de la amenaza Vs. crecimiento tecnológico (Fuente: Elaboración propia)

Teniendo en cuenta los datos presentados en la Tabla 1 y graficados en la Figura 6, se puede observar que el aumento en la cantidad de incidentes informáticos presentados entre el 2009 y el 2015 es proporcional a la aparición de nuevas familias de malware que se ha dado en el mismo periodo; de igual forma, se observa que el crecimiento de la industria de la ciberseguridad se ha dado en una pendiente mucho más pronunciada.

De los anterior, se pude concluir que el crecimiento generado por la industria de la Ciberseguridad no ha generado una disminución en la aparición de nuevas familias de malware ni en los incidentes informáticos, como se hubiera esperado; por lo cual se puede determinar que las nuevas tecnologías, de forma global, no han sido eficientes en mitigar los crecientes riesgos que se encuentran latentes en el ciberespacio.

4.5. TENDENCIA DE LAS AMENAZAS CIBERNÉTICAS

Lo más grave de toda esta situación no es el crecimiento de la amenaza o el aumento en la cantidad de incidentes cibernéticos reportados, lo preocupante de todo esto es la afectación que todo esto está generando para las diferentes entidades y organizaciones, tanto de tipo público como privado. El impacto generado por esto se puede apreciar en el último informe de la empresa Gemalto, denominado "Las malas prácticas de seguridad interna cobran un peaje" (Poor Internal Security Practices Take a Toll), en dicho informe se aprecian la afectación real en cifras contra los diferentes tipos de organizaciones y entidades. A continuación, se presentan algunas de las cifras más relevantes de dicho informe [7].

Dicho informe comienza con cifras tan contundentes como alarmantes, ya que, según las estadísticas recopiladas, durante la primera mitad del 2017 diferentes organizaciones en el mundo habrían visto vulnerada su seguridad informática permitiendo el robo de 1.901'866.611 registros de información, cifra que por sí sola es muy preocupante, pero que se hace aún más grave, cuando dicha información es complementada con el siguiente cálculo de robos de registros de información [7]:

- Cada día se pierden 10'507.550 registros de información
- Cada hora se pierden 437.815 registros de información
- Cada minuto se pierden 7.297 registros de información
- Cada segundo se pierden 122 registros de información

Según el mismo informe, "mientras muchas organizaciones se han enfocado en detectar y detener amenazas externas, las amenazas internas – atacantes internos, pérdida accidental y otros tipos de negligencia – pueden ser riesgos olvidados"; esto nos indica que las estrategias de seguridad digital adoptadas por la mayor parte de las entidades y organizaciones, tanto de tipo público como privado, han dirigido la mayor parte de su esfuerzo en robustecer la seguridad perimetral asumiendo que la mayor parte de los riesgos y los más relevantes están por fuera de las estructuras informáticas propias.

4.6. PRESUNCIÓN DE LA BRECHA

Las estrategias de ciberseguridad que se basaban en el paradigma de defensa en profundidad validaban el tipo de estrategias que venían siendo utilizadas hasta la actualidad; sin embargo, desde hace pocos años se ha venido fortaleciendo un nuevo paradigma denominado "presunción de la brecha" (assumption of breach). Según esta nueva teoría, y como su nombre lo indica, las estrategias de ciberseguridad modernas deben basarse en la presunción de la brecha de seguridad, en otras palabras se debe asumir que el mayor riesgo proviene del interior de la red y no del exterior como había sido manejado hasta ahora.

Según la Compañía Atrion, en su documento denominado “Assumption of Breach a New Approach to Cyber Security”, la ciberseguridad de una organización se sostiene sobre tres pilares fundamentales [8]:

1. Personas

2. Políticas

3. Tecnología

Según el mismo documento, las personas que podrían afectar la seguridad de las redes informáticas de una organización desde el interior se dividen en cuatro grupos, los cuales se describen brevemente a continuación:

- Practicantes de Tecnologías de la Información: Este grupo de personas son las encargadas de interactuar directamente con diferentes tipos de tecnología y son los responsables por la seguridad de la infraestructura informática digital. Además textualmente el autor afirma que *"Si vemos el panorama de amenazas actual como un campo de batalla, los profesionales de TI son tus soldados; necesitan capacitación de alta calidad para ser efectivos, específicamente sobre cómo operar los sistemas de seguridad y las soluciones que la organización ha comprado*"; de igual forma manifiesta que *"En la mayoría de los casos, estas personas también se encargarán de aprovechar los procesos y tecnologías de la organización, por lo que es fundamental que tengan la capacitación y el conocimiento necesarios para hacerlo de manera efectiva"* [8].

- Empleados: Este es el grupo de personas que hacen uso de las tecnologías disponibles dentro de la organización para desarrollar sus actividades profesionales dentro de la misma. Usualmente dentro de este grupo de personas se incluyen aquellas que no tienen conocimientos profundos sobre la ciberseguridad y que por lo tanto deben ser protegidas por los sistemas destinados para tal fin dentro de la organización y deben ser educados sobre los diferentes tipos de amenazas cibernéticas, teniendo en cuenta que este grupo representa la parte más vulnerable para la ciberseguridad de cualquier tipo de entidad [8].

- Líderes: Son las personas encargadas de dirigir los diferentes procesos de la organización, los cuales en algunos casos hacen parte de la junta directiva, y son quienes deben ayudar a crear la visión de la estrategia de ciberseguridad que se diseñe para la institución a la que pertenecen; por lo que el éxito de la misma depende en gran parte de estas personas [8].

- Consultores externos: Son personas o empresas ajenas a la organización, que prestan algún tipo de asesoría a los equipos encargados de las TIC’s dentro de la organización.

Dentro del marco de una estrategia de ciberseguridad, se encuentra que dentro de los tres primeros grupos: Practicantes de Tecnologías de la Información, Empleados y Líderes; se encuentran las personas que podrían impactar directamente en la ciberseguridad de una organización. Teniendo en cuenta las descripciones de estos grupos de personas, se encuentra que existe un factor común a los 3 que podría impactar positivamente de forma relevante dentro de la ciberseguridad de cualquier tipo de organización, dicho factor es la educación [8].

5. METODOLOGÍA

El desarrollo del presente proyecto se ha sustentado en un enfoque de investigación cuantitativa [9], mediante el cual se busca identificar las cusas que han llevado a que las tecnologías aplicadas a la ciberseguridad de las organizaciones no hayan llevado a la disminución sustancial de los incidentes de seguridad y pérdidas de información que en la actualidad vienen enfrentando. Partiendo de la identificación de dichas causas se pretende plantear una solución, basada en el fortalecimiento de la educación de los usuarios de las redes y sistemas, que conlleve a disminuir el impacto generado dentro de las organizaciones por las amenazas cibernéticas y que facilite la medición de sus resultados.

5.1. PREGUNTAS DE INVESTIGACIÓN

- ¿Cuáles son las principales amenazas cibernéticas que enfrentan los usuarios y cómo se podrían clasificar?

- Desde la perspectiva del usuario de las redes y sistemas informáticos de una organización ¿Cuáles son los factores que dan origen o facilitan el accionar de las amenazas cibernéticas?

- Desde un proceso educativo ¿cómo se puede contribuir a disminuir la probabilidad de que las amenazas cibernéticas se materialicen dentro de las organizaciones por acciones de los usuarios?

5.2. PLANTEAMIENTO DEL PROBLEMA

Como se ha visto hasta este punto, las estrategias adoptadas por la humanidad en general para hacer frente al crecimiento de las amenazas cibernéticas no han impactado en la forma en que se esperaría que lo hubieran hecho. Esto ha obligado a que las personas encargadas de estudiar, analizar y entender el ciberespacio y las diferentes amenazas latentes dentro del mismo, hayan estructurado diferentes principios sobre los cuales de forma general se han venido constituyendo las estrategias de ciberseguridad adoptadas por la mayor parte de las organizaciones.

Tal vez uno de los principios más utilizados hasta el momento, es el principio de defensa en profundidad, bajo el cual se fortalece la seguridad perimetral de las organizaciones mediante la implementación de tecnologías de protección, las cuales buscan hacer más robusto el perímetro de las redes, pero que descuidarían la seguridad interna de las mismas.

Por lo anterior, recientemente se ha establecido un nuevo principio que ha tenido mucha acogida, el cual disminuye la importancia de la seguridad perimetral, dándole prioridad a la seguridad interna de las redes informáticas de las organizaciones. Bajo este nuevo paradigma se ha señalado al usuario final de las redes como la parte más vulnerable, para la

ciberseguridad de una organización, y sobre la cual las tecnologías actuales no tendrían el efecto deseado.

El problema entonces gira alrededor de la relevante vulnerabilidad generada por los usuarios de las redes informáticas digitales de una organización y su solución debería estar orientada a la mitigación de los riesgos generados por dicho factor humano.

6. OBJETIVOS

Con el fin de abordar la problemática planteada, se estructurará el siguiente proyecto, mediante el cual se busca analizar las principales amenazas cibernéticas, con el fin de identificar los factores de riesgo que se encuentran vinculados a los usuarios, facilitando la materialización de dichas amenazas; partiendo de dicho análisis se estructurarán las bases para un plan de sensibilización que pueda ser implementado en la mayor parte de las organizaciones, con el fin de disminuir las facilidades que brindan los usuarios finales de los sistemas TIC dentro de las organizaciones, muchas veces por desconocimiento o ignorancia sobre los peligros latentes en el ciberespacio.

Para dar cumplimiento a lo anterior se han planteado los siguientes objetivos dentro del alcance del presente proyecto:

6.1. OBJETIVO GENERAL

Diseñar un programa de sensibilización que pueda ser orientado a la mayor parte de usuarios de la red (con conocimiento técnico o sin él), de forma tal que dicho programa se constituya en una medida adicional dentro de un programa de seguridad.

6.2. OBJETIVOS ESPECÍFICOS

- Determinar los principales tipos de amenazas cibernéticas a las que se encuentran expuestos la mayor parte de los usuarios.

- Identificar los principales focos de riesgo que generan los grupos de amenazas determinados en el punto anterior.

- Diseñar un programa de sensibilización mediante el cual se conduzca a eliminar los comportamientos y malas prácticas que aumentan el nivel de riesgo dentro de una organización.

7. TAXONOMÍA DE LAS AMENAZAS

Como parte relevante del análisis, se hace necesario realizar una identificación de las principales amenazas cibernéticas, clasificándolas en ciertos grupos que reúnan características similares, de forma que se facilite sus análisis. Por lo anterior; antes de iniciar con el trabajo propio del presente capitulo, se empezará seleccionando una definición de amenaza que se acerque a las necesidades del trabajo que se viene adelantando.

Según el diccionario de la lengua española se define amenaza como aquel delito consistente en intimidar a alguien con el anuncio de la provocación de un mal grave para él o su familia[1]. De la definición anterior, se resalta la importancia de que una amenaza representa un "peligro latente"; esto quiere decir que una amenaza podría ser el origen de una situación que llegara afectar, en este caso, la infraestructura informática digital de cualquier tipo de organización; por lo cual las amenazas cibernéticas se constituirían en la raíz de cualquier tipo de afectación que se origine en o a través del ciberespacio y con base en este principio se hace indispensable reconocer plenamente su estructura para diseñar estrategias que permitan mitigar o controlar los riesgos generados por su existencia.

Al igual que cualquier tipo de amenaza, las cibernéticas están evolucionando y una de las razones particulares es que, como se indicó en el capítulo anterior, en la actualidad la sociedad se ha visto abocada al uso masivo de herramientas tecnológicas; esta dependencia tecnológica, ha generado un aumento considerable en lo que se conoce como la "Superficie de Ataque[2]", llevando a que uno de los objetivos más expuestos sea la información producida y gestionada por los diferentes tipos de organizaciones; esto ha llevado a que en la actualidad la información sea considerada como uno de los activos más importantes para la mayor parte de las organizaciones.

De la mano de lo expuesto anteriormente, se resalta el estrecho vínculo que existe en la actualidad entre la información y las TIC's, teniendo en cuenta que estas últimas juegan un papel relevante en todas y cada una de las fases del ciclo de vida de la información:

- Generación
- Selección
- Representación
- Almacenaje

[1] Tomado de http://dle.rae.es/?w=diccionario

[2] La superficie de ataque de IoT es la suma total de todas las vulnerabilidades potenciales de seguridad en dispositivos IoT, y el software y la infraestructura asociados en una red dada, ya sea local o en toda la internet. (Fuente: http://searchdatacenter.techtarget.com/es/definicion/Superficie-de-ataque-de-IoT)

- Recuperación
- Distribución
- Uso

Este vínculo ha generado la necesidad de que las organizaciones se esfuerzan en:

- Generar valor para la organización mediante inversiones en Tecnologías de la Información y las Comunicaciones (TIC's).
- Perseguir la excelencia operativa a través de una aplicación de la tecnología fiable y eficiente.
- Mantener en un grado aceptable los riesgos relacionados con TIC's.
- Cumplir con las regulaciones legales, regulaciones, acuerdos contractuales y políticas aplicables, especialmente aquellas relacionadas con la protección de datos.

Los ejes de esfuerzo plasmados anteriormente, hacen que sea necesario considerar los riesgos que giran alrededor de la información gestionada a través de las TIC's, esfuerzo que partirá del análisis en profundidad que se realice a las principales amenazas a las cuales se encuentran expuestas la mayor parte de las organizaciones, trabajo que se realizará sobre una estructuración taxonómica.

El objetivo de dicha taxonomía es establecer un punto de referencia para las amenazas cibernéticas, que facilite analizar e identificar los orígenes de cada grupo establecido, de forma que dicho análisis permita diseñar estrategias orientadas a mitigar y controlar los riesgos generados. En particular esta taxonomía se constituirá en una estructura viva que se utilizará para mantener una visión coherente de las amenazas cibernéticas sobre la base de la información recopilada. Para el presente trabajo se considera que la taxonomía de las amenazas cibernéticas se puede identificar en un ambiente que permita clasificarlas en tres grandes clases o tipos, como son: ataque de red, ataque de equipo de cómputo y ataque de aplicación, a continuación se describe algunos de estos componentes de estas tres (3) clases.

7.1. ATAQUE DE RED

En esta fase se ubican todos y cada uno de los elementos que tiene que una característica que representa la colección de computadoras y otros hardwares conectados por canales de comunicación para compartir recursos e información. A medida que la información viaja de un sistema a otro a través del canal de comunicación, una persona malintencionada puede entrar en el canal de comunicación y robar la información que viaja a través de la red.

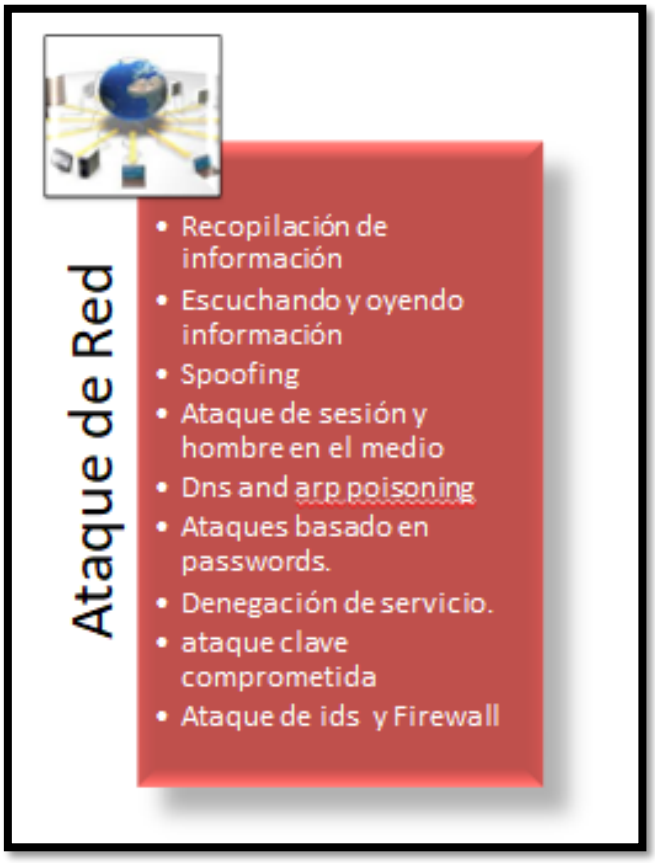

Figura 7 - Ataque de RED (Fuente: Adaptación módulo 1 CEH EC Council)

7.1.1. Recopilación de Información

La recopilación de información es la primera fase en el proceso de prueba de penetración. El objetivo principal de la recopilación de información es comprender más acerca de la empresa objetivo. Hay varias formas de recopilar información sobre la empresa de fuentes de dominio público, como internet, periódicos y fuentes de información de terceros.

7.1.2. Sniffing and eavesdropping

El rastreo de paquetes o sniffing es un proceso de monitoreo y captura de todos los paquetes de datos que pasan a través de una red determinada usando una aplicación de software o un dispositivo de hardware. El rastreo es sencillo en redes basadas en concentradores ya que el tráfico en un segmento que pasa por todos los hosts asociados con ese segmento.

Sin embargo, la mayoría de las redes actuales se comunican a través de switches, estos son dispositivos de red que se encargan de darle direccionamiento a los paquetes de información que transitan entre los diferentes dispositivos de la red; además de este tipo de dispositivos, existe lo que se conoce como un hub, la diferencia entre este último y un switch es que un hub transmite datos de línea a cada puerto de la máquina y no tiene asignación de línea, mientras que el swithc observa la dirección de control de acceso de medios asociada a cada

cuadro que pasa por él y envía los datos al puerto requerido mediante la dirección MAC del dispositivo asociado (Una dirección MAC es una dirección de hardware que identifica de manera única cada nodo de una red).

Para el desarrollo exitoso de esta técnica, un atacante necesita manipular la funcionalidad del conmutador para ver todo el tráfico que pasa por él; para ello podría acudir a un programa de sniffing, mediante el cual podría capturar paquetes de datos solo dentro de una subred dada.

Un atacante que realice actividades de eavesdropping o escucha a escondidas en este dominio de difusión de capa 2 no protegido, puede responder a la solicitud ARP de difusión, y responde al remitente mediante spoofing de la dirección IP del destinatario, el atacante ejecuta un sniffer y convierte el adaptador NIC de la máquina en modo promiscuo.

7.1.3.Spoofing

El spoofing[3] es una técnica que los hackers realizan con alguna frecuencia para tener la identidad o el acceso robada, cuando una persona simula ser otra persona, organización o empresa con el propósito de obtener acceso a información personal confidencial, dentro los que se encuentran datos confidenciales como cuentas bancarias y números de tarjetas de crédito. Existen algunos tipos conocidos de suplantación de identidad como: suplantación de IP, suplantación de URL, suplantación de correo electrónico, suplantación de DNS y suplantación de MAC.

7.1.4.Session Hijacking and Man-in-the-Middle attack

Un servidor web envía un token de identificación de sesión o clave a un cliente web después de la autenticación exitosa del cliente. Estos tokens de sesión diferencian varias sesiones que el servidor establece con varios clientes. Los servidores web usan varios mecanismos para generar tokens aleatorios y varios controles para asegurarlos durante la transmisión a los clientes.

Un ataque de secuestro de sesión hace referencia a la explotación de un mecanismo de generación de token de sesión o controles de seguridad de token, de modo que el atacante puede establecer una conexión no desatinada con un servidor de destino. El atacante puede adivinar o robar una ID de sesión válida (que identifica a los usuarios autenticados) y la usa para establecer una sesión con el servidor. El servidor web responde a las solicitudes del atacante como si estuviera comunicándose con un usuario autenticado.

Los atacantes pueden usar el secuestro de sesión para lanzar varios tipos de ataques como el de hombre en el medio y ataques de Dos. Un ataque MITM es aquel que el atacante se coloca entre el cliente y los servidores. El secuestro de sesión permite a los atacantes ubicarse entre

[3] Tomado de https://pecb.com/pdf/articles/38-pecb_security-vs-spoofing.pdf

el cliente autorizado y el servidor web, de modo que toda la información, viajando en cualquier dirección, debe atravesarlos. El navegador del cliente cree que se está comunicando directamente con el servidor, y el servidor cree que se está comunicando directamente con el cliente autorizado; sin embargo, todo el tráfico entre los pases a través del atacante. Los atacantes pueden realizar sniffing de toda la información confidencial de la sesión e interrumpir las sesiones para provocar un ataque de denegación de servicio.

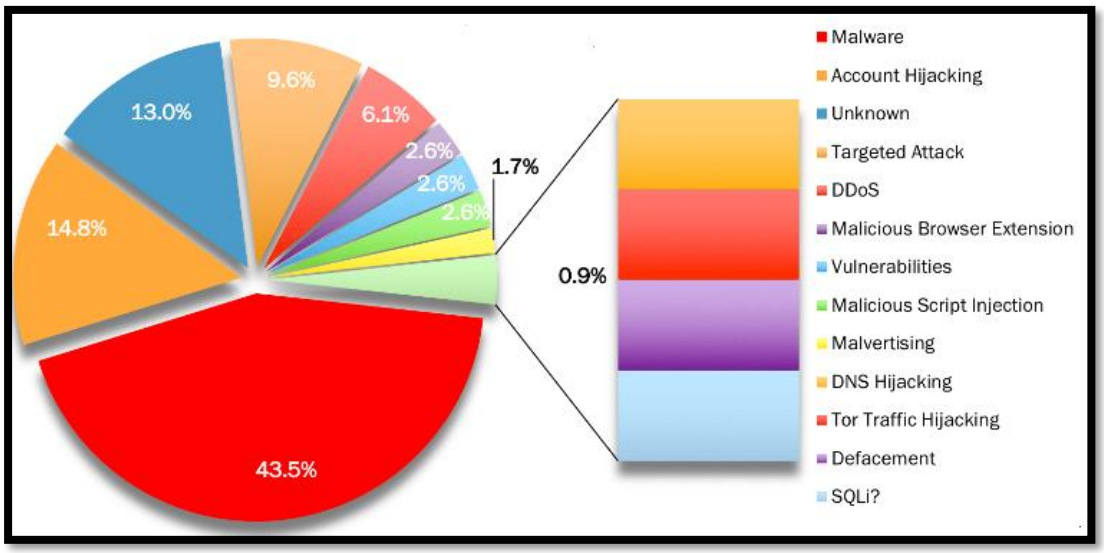

Figura 8 - Técnicas de Ataque a Enero 2018 (fuente: ww.hackmageddon.com/2018)

El secuestro de cuenta es un tipo de ataque de secuestro de sesión en el que el atacante roba el correo electrónico, la computadora u otro tipo de información de la cuenta del usuario. El atacante podría usar la información robada para actividades maliciosas. En enero de 2018, el secuestro de cuentas adquirió el segundo lugar en la lista de las técnicas de ataque más frecuentemente utilizadas, con una tasa de concordancia del 14.8%, después de la técnica de malware.

7.1.5. Denial-of-Service attack

En un ataque de denial-of-service (DoS), un atacante sobrecarga los recursos de un sistema, derribando el sistema o al menos disminuyendo significativamente el rendimiento del sistema; el objetivo de un ataque de Dos no es obtener acceso no autorizado a un sistema, su razón es evitar que los usuarios legítimos usen el sistema.

Los siguientes son ejemplos de tipos de ataques Dos:

- Flooding o inundación de datos a la víctima con más tráfico de lo que se puede manejar.
- Bloquear una pila TCP / IP enviando paquetes corruptos.
- Estrellar un servicio al interactuar de una manera inesperada.

- Hanging o colgando de un sistema haciendo que entre en un ciclo infinito.

Los ataques DoS vienen en una variedad de formas y se dirigen a una variedad de servicios. Los ataques pueden causar lo siguiente:

- Consumo de recursos escasos y no renovables.
- Consumo de ancho de banda, espacio en disco, tiempo de CPU o estructuras de datos.
- Destrucción física real o alteración de los componentes de la red.
- Destrucción de programación y archivos en un sistema informático.

7.2. ATAQUE DE EQUIPO DE CÓMPUTO

En esta clase se ubican los elementos cuya característica representan se dirigen a un sistema particular en el que reside la información valiosa. Los atacantes intentan violar la seguridad del recurso del sistema de información.

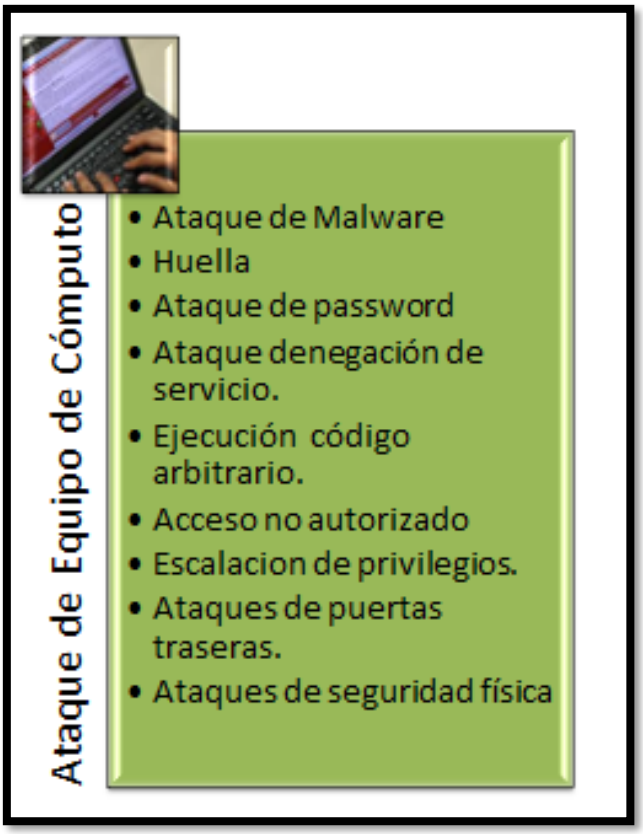

Figura 9 - Ataque de Equipo de Cómputo (Fuente: Adaptación módulo 1 CEH EC Council)

7.2.1. Ataques de Malware

El malware es un software malicioso que daña o deshabilita los sistemas informáticos y otorga un control limitado o total de los sistemas a su creador con fines de robo o fraude. Entre los principales tipos de malware se incluyen virus, gusanos, troyanos, rootkits, spyware, etc.; su ejecución en una máquina víctima puede generar diferentes tipos de efectos, entre los que se destaca que pueden eliminar archivos, volver lentos la velocidad de las computadoras, robar información personal, enviar spam y cometer fraudes.

El malware tiene la capacidad de realizar diversas actividades maliciosas que van desde la simple publicidad por correo electrónico hasta el robo de identidad complejo y el robo de contraseñas.

Los programadores de malware lo desarrollan y lo usan para:

- Atacar navegadores y rastrear sitios web visitados.
- Afectar el rendimiento del sistema, haciéndolo muy lento.
- Causar fallas de hardware, haciendo que las computadoras no funcionen o lo hagan de forma errada.
- Robar información personal, incluidos los contactos.
- Borrar información importante, lo que da como resultado pérdidas de datos potencialmente enormes.
- Atacar a sistemas informáticos adicionales, directamente desde un sistema comprometido.
- Comprometer los sistemas de correo electrónico mediante las bandejas de entrada, inundándolas de spam con correos electrónicos publicitarios.

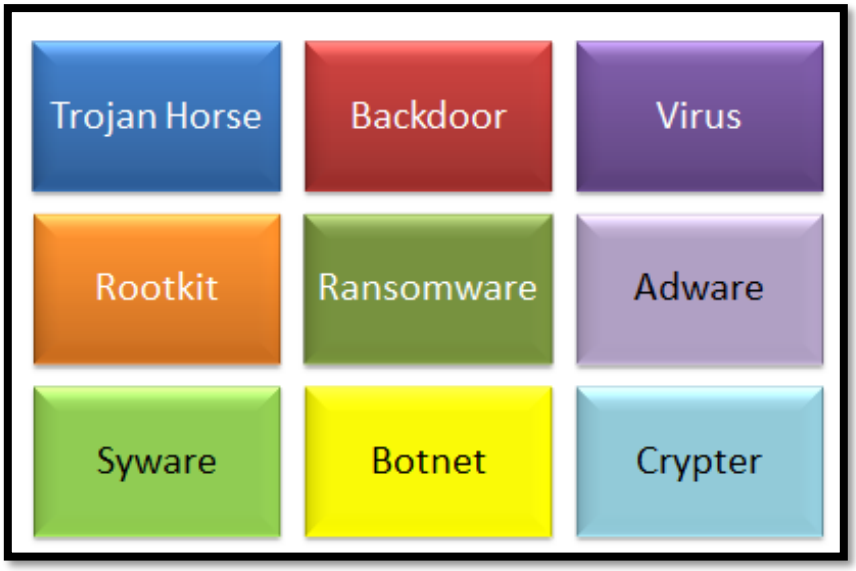

Figura 10 - Algunos ejemplos de Malware (Fuente: Adaptación módulo 6 CEH EC Council)

7.2.2. Seguimiento de Huellas - Footprinting

Los atacantes ejecutan el seguimiento de huellas como el primer paso de cualquier ataque a los sistemas de información. En la fase de footprinting, los atacantes intentan extraer valiosa información a nivel del sistema, como detalles de la cuenta, sistema operativo y otras versiones de software, nombres de servidores, detalles del esquema de la base de datos, etc. que serán útiles durante el resto del proceso de hacking.

Las siguientes son varias amenazas generadas por el desarrollo de técnicas de footprinting:

Figura 11 - Amenazas del Footprinting (Fuente elaboración propia)

7.2.2.1. Ingeniería Social

Sin utilizar ningún método de intrusión, los piratas informáticos recopilan información directa e indirectamente a través de la persuasión y de otros medios. Aquí, los hackers recopilan información crucial de empleados dispuestos que no están conscientes de la intención de los hackers.

7.2.2.2. Ataques de sistema y red

El footprinting ayuda a un atacante a planear y facilita la ejecución posterior de ataques contra los sistemas y las redes, posterior al despliegue de esta técnica se facilitará la identificación y análisis de vulnerabilidades, que conllevará a la identificación de las posibles vías de acceso a la infraestructura víctima, lo que conllevará a la prueba de cada una de esas opciones para el atacante las cuales se materializan mediante el despliegue de ataques contra los sistemas y las redes que facilitan su comunicación, lo que concluirá con la manipulación total o parcial de la infraestructura digital.

7.2.2.3. Fuga de Información

La fuga de información puede suponer un problema para cualquier organización que caiga en manos de los atacantes, pueden construir un plan de ataque basado en la información, o usarlo para un beneficio monetario.

7.2.2.4. Pérdida de privacidad

Todas las organizaciones necesitan y deben mantener parte de su información de forma privada, lo anterior en busca de proteger datos que puedan ser utilizados para afectar el desarrollo de las actividades normales de cualquier tipo de entidad (pública o privada); gracias al uso de las TIC's, hoy en día la mayor parte de esta información se encuentra almacenada en sistemas digitales y puede ser accedida a través del ciberespacio. Lo anterior ha generado que los atacantes busquen identificar los puntos de acceso de dicha información y enfoquen su esfuerzo en vulnerar los sistemas de seguridad, de forma que puedan llegar a obtener, destruir o manipular dicha información.

7.2.2.5. Espionaje corporativo

El espionaje corporativo es una de las principales amenazas para las organizaciones, ya que los competidores pueden espiar e intentar robar datos confidenciales a través del desarrollo de diferentes tipos de técnicas. Esta técnica puede redundar en pérdidas económicas considerables que se generen por competencia desleal, por ejemplo, una empresa podría lanzar productos de una organización víctima similares en el mercado, lo que afecta la posición de mercado de una organización objetivo.

7.2.2.6. Pérdida comercial.

Otro de los ataques importantes a los que se encuentran expuestas las organizaciones, sobre todo aquellas que realizan negocios en línea, comercio electrónico, negocios bancarios y financieros relacionados, etc.; podría generar pérdidas considerables de dinero, si su seguridad se ve vulnerada durante el desarrollo de este tipo de operaciones.

7.2.3. Password attacks

A través de diferentes técnicas los atacantes adelantan esfuerzos que les permitan conseguir el acceso a las diferentes plataformas tecnológicas; uno de los medios más comunes que permiten dicho objetivo es conociendo la contraseña, por lo que este sistema de autenticación se ve expuesto a diferentes tipos de ataques.

Uno de los más utilizados es la fuerza bruta, la cual suele combinarse con un ataque de diccionario, en el que se encuentran diferentes palabras para ir probando con ellas, por lo que

es muy importante que los usuarios fortalezcan o hagan más robustas sus contraseñas, de forma que se les dificulte el desarrollo de este tipo de técnicas a los atacantes.

7.2.4. Arbitrary code Execution

Este concepto de ejecución arbitraria de código, se conoce como la capacidad que tiene los atacantes para ejecutar comandos o inyectar código en una aplicación, por lo general haciendo uso de una vulnerabilidad que este tiene, tal es el caso del desbordamiento de buffer lo cual ocurre cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer).

7.2.5. Unauthorized access

Mediante el desarrollo de esta técnica un atacante logra obtener acceso a un sistema haciendo uso de la cuenta o credencial de otro usuario o persona que tenga derecho de entrar al sistema.

En algunas plataformas tecnológicas se configuran para generar alertas para avisarles a los responsables de la administración de los sistemas, cuando un usuario realiza varios intentos para entrar a los sistemas permitiendo la investigación de lo ocurrido, de igual forma existen plataformas tecnológicas que bloquean las cuentas de los usuarios, lo que en cierta forma puede ayudar a mitigar un poco el riesgo.

7.2.6. Backdoor attacks

Los ataques de puerta trasera o backdoor son programas que se almacenan en los sistemas operativos con el propósito de tener acceso. Los atacantes utilizan este tipo de técnicas sin la detección del usuario, le ayudan a los atacantes a obtener acceso no autorizado a un sistema remoto y realizar actividades maliciosas.

El objetivo del backdoor es obtener privilegios de root en un sistema, al iniciar sesión como el usuario raíz de un sistema, un atacante puede realizar cualquier tarea, como instalar software o eliminar archivos, y así sucesivamente.

7.3. ATAQUE DE APLICACIÓN

Las aplicaciones pueden ser vulnerables, si no se toman medidas de seguridad adecuadas al desarrollarlas, implementarlas y mantenerlas. Los atacantes explotan las vulnerabilidades presentes en una aplicación para sellar o destruir datos.

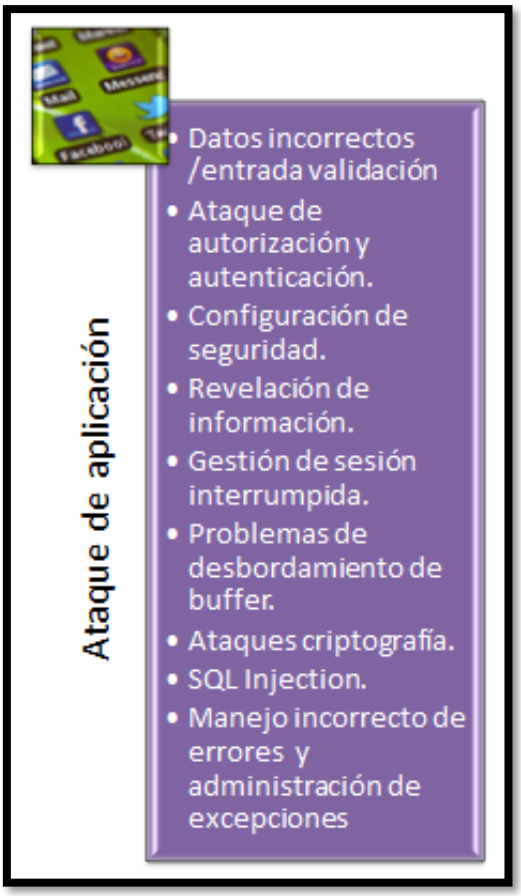

Figura 12 - Ataque de Aplicación (Fuente: Adaptación módulo 1 CEH EC Council)

7.3.1. Seguridad de configuración

La línea base de cualquier componente tecnológico permite una descripción de configuración base que se debe tener, este método es necesario para tener los aspectos mínimos de configuración que se ajusta de acuerdo a los requerimientos funcionales.

Sin esta configuración predeterminada y aprobada por los responsables de seguridad, es fácil que los atacantes desarrollen nuevas formas de realizar ataques a dichos sistemas, normalmente este método no es adaptado por las organizaciones.

7.3.2. Revelación de información

Dentro de la técnica de revelación de información se encuentra los metadatos la cual permite suministrar información sobre los datos producidos. Esta información describe el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos.

En algunos casos esta técnica permite a los atacantes ubicar y entender los datos, incluyen información requerida para determinar los objetivos del vector de ataque

7.3.3. Ataques de criptografía

La criptografía es la práctica de ocultar información convirtiendo el texto del plan (formato legible) en texto de cifrado (formato ilegible) usando una clave o esquema de cifrado. La criptografía protege los datos confidenciales, como los mensajes de correo electrónico, las sesiones de chat, las transacciones web, los datos personales, las aplicaciones de comercio electrónico de datos corporativos y muchos otros tipos de comunicación.

Los mensajes cifrados pueden descifrarse en el momento mediante criptoanálisis (descifrado de código) aunque las técnicas de cifrado modernas son prácticamente irrompibles.

7.3.3.1. Objetivos de la criptografía

- ***Confidencialidad:*** *garantía de que la información solo es accesible para aquellos autorizados a tener acceso.*

- ***Integridad*****:** indica la confiabilidad del documento o cualquier dato que garantice la calidad de ser genuino. o recursos en términos de prevenir cambios impropios y no personalizados

- ***Disponibilidad:*** *Significa garantizar que todos los servicios informáticos se encuentren disponibles para los diferentes usuarios que lo requieran.*

- ***No repudio:*** garantice que el remitente de un mensaje no puede luego negar haber enviado el mensaje, y que el destinatario no puede denegar haber recibido el mensaje.

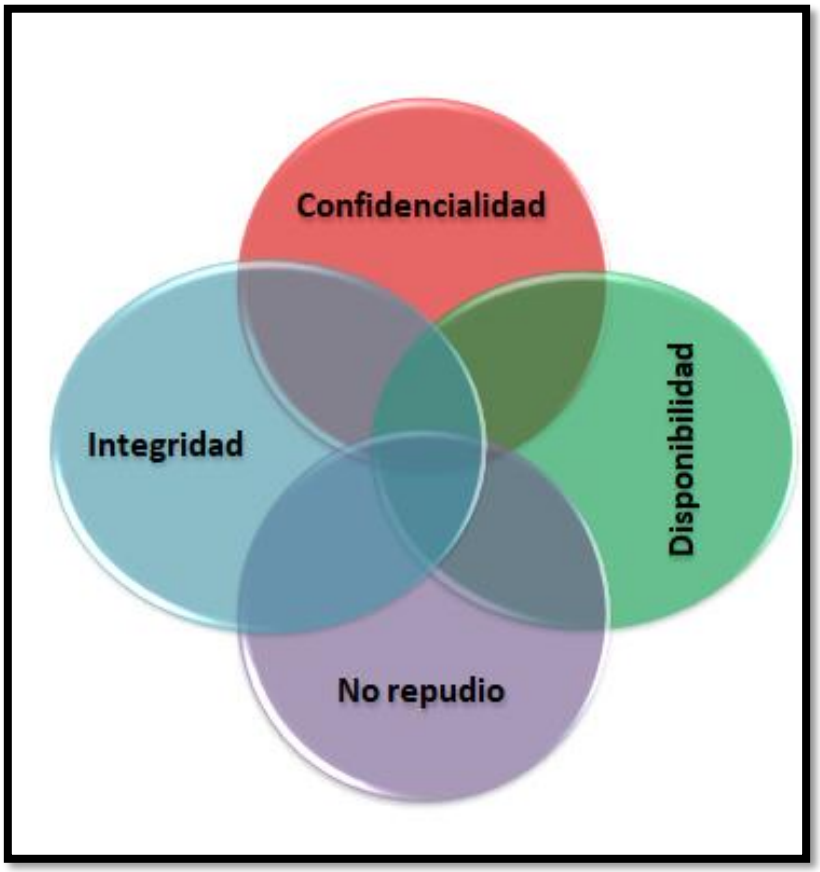

Figura 13 - Objetivos de la Criptografía (Fuente Elaboración Propia)

7.3.4.SQL injection

La inyección SQL es el ataque más común y devastador que los atacantes pueden lanzar contra un sitio web. Los atacantes usan varias técnicas y trucos para comprometer las aplicaciones de datos manejadas por los usuarios, y estos ataques generan grandes pérdidas para las organizaciones en términos de dinero. Reputación, pérdida de datos y pérdida de la funcionalidad.

Este tipo de ataque ha tenido un avance significativo en contra de las aplicaciones web, posicionándose en un segundo lugar con un 16.1%, según www.hackmageddon.com

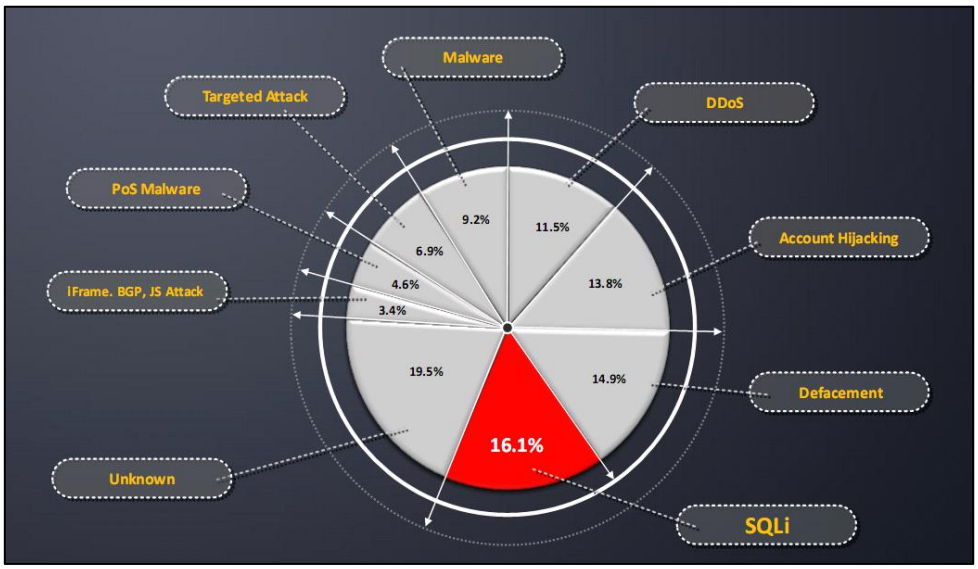

Figura 14 - Ataque de Aplicación (Fuente: módulo 13 CEH EC Council)

Structured Query Language (SQL) es un lenguaje de texto utilizado por un servidor de base de datos. Los comandos SQL que se utilizan para realizar operaciones en la base de datos incluyen INSERTAR, SELECT, UPDATE y DELETE. Los programadores usan estos comandos para manipular datos en el servidor de la base de datos.

Los programadores usan comandos SQL secuenciales con parámetros proporcionados por el cliente, lo que facilita a los atacantes la inyección de comandos. Los atacantes intentan ejecutar consultas SQL aleatorias en un servidor de base de datos a través de una aplicación web.

Los ataques de inyección SQL no explotan una vulnerabilidad de software específica, sino que se dirigen a sitios web que no siguen las prácticas de codificación segura para acceder y manipular los datos almacenados en una base de datos relacional.

Las tecnologías del lado del servidor implementan la lógica empresarial en el lado del servidor, que luego atiende las solicitudes entrantes de los clientes. La tecnología Sever-side accede sin problemas, entrega, almacena y restaura información. Varias tecnologías del lado del servidor incluyen ASP, ASP.net, Cold Fusion, JSP, PHP, Python, etc. Algunas de estas tecnologías son propensas a las vulnerabilidades de inyección de SQL, y las aplicaciones desarrolladas usando estas tecnologías son vulnerables a ataques de inyección de SQL. La aplicación web usa varias tecnologías de bases de datos como parte de su funcionalidad. Algunas bases de datos relacionales utilizadas para desarrollar aplicaciones web incluyen Microsoft SQL Server, Oracle, IBM DB2 y open-source MYSQL. Los desarrolladores a veces ignoran las prácticas de codificación segura cuando utilizan estas tecnologías, lo que hace que las aplicaciones sean vulnerables a los ataques de inyección SQL.

8. FACTORES DE RIESGO

Teniendo en cuenta las principales amenazas cibernéticas identificadas y clasificadas previamente; a continuación, se pretende determinar las principales causas que dan origen o facilitan la materialización de dichas amenazas contra las organizaciones, las cuales son generadas en su mayor parte por el desconocimiento de los usuarios de las redes y sistemas informáticos.

Teniendo en cuenta lo anterior, se han especificado los siguientes factores de riesgo que giran en torno a las prácticas de los usuarios relacionadas con el uso de las redes y sistemas informáticos.

8.1. USO INADECUADO DE LAS REDES SOCIALES

Las redes sociales en la actualidad de han constituido en verdaderos motores de investigación que permiten obtener información de las personas, afectando de esta manera la seguridad de las mismas; no obstante, ese peligro puede trascender a la afectación de la seguridad de las organizaciones a las cuales pertenecen los usuarios de dichas redes, ya que muchas personas no saben distinguir entre la información que debe ser privada y mantenerse como tal de aquella que puede hacerse pública.

A continuación, se puede evidenciar un sencillo ejemplo relacionado con esta falencia, imaginemos por un momento que somos atacantes y queremos obtener información sobre una empresa como por ejemplo Renault, para ello queremos identificar a las personas que trabajan en dicha compañía y lanzarles un ataque tipo “Spear Phishing”, para ello deberíamos identificar a las personas que trabajan en dicha compañía para realizar un ataque masivo con el fin de aumentar las probabilidades de éxito. Realizando una sencilla búsqueda a través de medios abiertos encontraríamos lo siguiente:

a. Lo primero que se realizaría es identificar a través de una red social, que personas trabajan en dicha empresa.

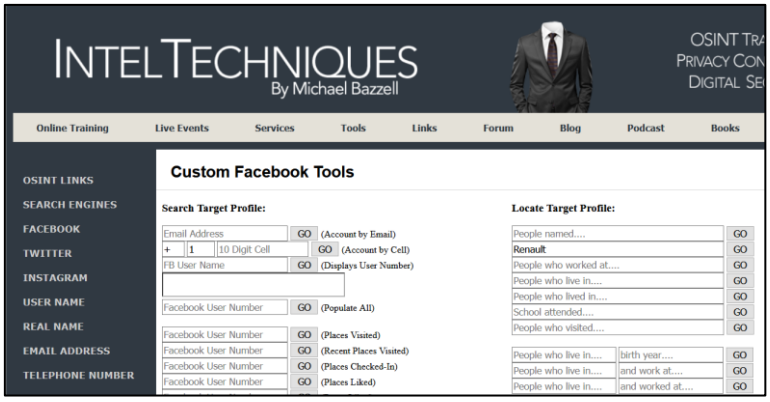

Figura 15 - Identificación de perfiles que trabajen en Renault (Fuente: Elaboración propia mediante el uso de la plataforma OSINT Framework)

b. Con la aplicación de este criterio de búsqueda mediante el uso de herramientas de la plataforma OSINT Framework se obtiene un listado de personas que trabajan para la supuesta compañía objeto del ataque.

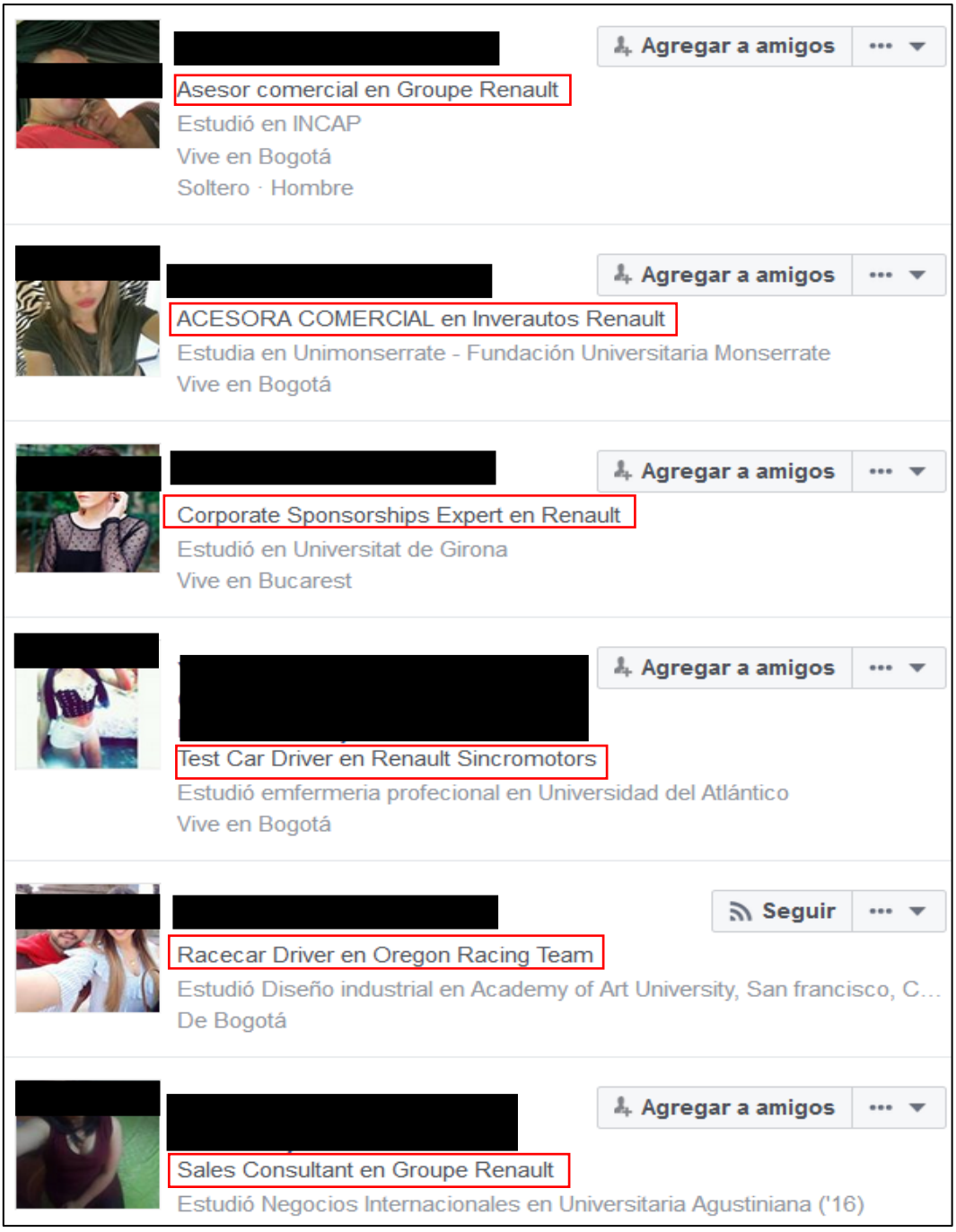

Figura 16 - Resultados de un ejemplo de búsqueda de personas miembros de una compañía (Fuente: Elaboración propia mediante consulta en Facebook)

c. Con los resultados de la información obtenida a través de redes sociales como se muestra en el ejemplo, se podría conocer un poco más sobre el perfil de las personas identificadas y diseñar un ataque tipo "Spear Phishing", que tenga mayores probabilidades de éxito.

   Lo anterior es sólo una pequeña muestra de lo que se puede realizar mediante la obtención de información publicada por usuarios en redes sociales, las cuales facilitan identificar a un grupo de personas miembros de una organización y en algunos casos hast identificar el cargo que ocupan dentro de la misma.

8.2. MAL MANEJO DE LA POLÍTICA BYOD (BRING YOUR OWN DEVICE)

Existe una política adoptada por muchas organizaciones hoy en día, la cual se denomina "Trae tu propio dispositivo" (*Bring Your Own Device*), a través de la cual se autoriza que los empleados de las organizaciones ingresen sus dispositivos portátiles a las instalaciones y se conecten con ellos a las redes de la organización para la realización de las actividades propias de su trabajo. Si bien esta puede ser una práctica que genera beneficios para la organización como para el usuario; de no ser bien administrada podría convertirse en un factor de riesgo relevante. Lo anterior se debe principalmente al descuido de las medidas de seguridad en los dispositivos personales de los usuarios, los cuales en gran parte de los casos se encuentran por fuera de los controles de seguridad implementados por la organización.

Estas características hacen que el manejo inadecuado de esta política pueda generar graves problemas para la seguridad de la infraestructura TI de la organización, ya que gran parte de la superficie de ataque de la misma estaría por fuera del control de seguridad implementado, generando una brecha para la infraestructura informática digital.

El factor de riesgo generado por la mala aplicación de esta política se resume a continuación:

Figura 17 - Riesgos asociados al BYOD (Fuente: traducción de la infografía disponible en https://www.welivesecurity.com/2012/04/04/byod-infographic-for-security-not-a-pretty-picture/)

La información contenida en la Figura 17 permite ver claramente como el mal manejo de una política diseñada para dar facilidades a los usuarios para la realización de sus actividades laborales, así como para disminuir los costos generados para la organización por adquisición y mantenimiento de equipos, puede generar un riesgo muy alto para la ciberseguridad de la misma si el usuario no administra de forma adecuada sus dispositivos personales.

8.3. CONEXIONES A REDES DE POCA CONFIANZA

Como se mencionó al inicio del presente documento, el ser humano ha generado un estrecho vínculo con la tecnología, lo que lo actualmente lo obliga a mantenerse conectado la mayor parte del tiempo a Internet, esto ha llevado a que la mayor parte de los usuarios busquen acceder a cualquier red sin evaluar los riesgos que esto puede implicar para la seguridad de la información que almacenan o transmiten desde los dispositivos que utilizan para establecer dichas conexiones.

Es así como hoy en día es muy común ver a las personas buscando redes Wi-Fi gratuitas, bien sea en aeropuertos, centros comerciales, restaurantes o cualquier tipo de red abierta la cual ofrece mínimas medidas de seguridad para los usuarios de la misma. El problema en sí no es el uso de estas redes, lo cual es muy riesgoso, sino la falta de tomar medidas de seguridad adicionales cuando se accede a este tipo de redes.

Según el portal británico *"Action Fraud"*, el acceso a este tipo de redes es bastante considerable, ya que el 76% de las personas que tienen un plan de datos aún utilizan redes Wi-Fi públicas, el 64% de ellas hace uso de las mismas desde cafés y bares, lo que implica que cada año se gasten más de 28 billones de minutos en el uso de este tipo de redes en Gran Bretaña.

Figura 18 - Estadísticas relacionadas con el uso de redes públicas (Fuente: https://www.actionfraud.police.uk/news/is-public-wi-fi-as-safe-as-you-think-jan16)

Según el mismo portal, otro aspecto relevante relacionado con este factor de riesgo es el incremento del uso de este tipo de redes; esto se ve reflejado en la tendencia al crecimiento de la cantidad de accesos de este tipo disponibles en Gran Bretaña, ya que para el 2014 existían aproximadamente 202.944 puntos de acceso y para el 2016 la suma llegaba a los 269.000 puntos disponibles aproximadamente.

Es importante resaltar que este tipo de redes en muchas ocasiones están protegidas por un firewall que blinda a los usuarios de estas redes de ataques que provienen del exterior de estas estructuras, sin embargo, no cuenta con medidas que permitan protegerse de los usuarios internos de dichas redes, lo que facilita ataques tipo "hombre en el medio" por ejemplo.

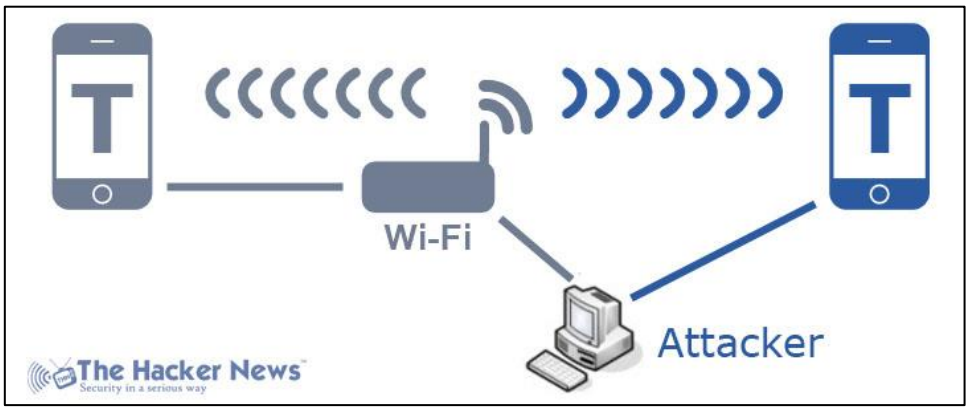

Figura 19 - Diagrama de un ataque tipo "Hombre en el Medio" (Fuente: https://thehackernews.com/2013/03/t-mobile-wi-fi-calling-app-vulnerable.html)

Si bien es cierto que muchas aplicaciones y protocolos hoy en día, implementan algoritmos de cifrado para proteger la información que se envía y se recibe por parte de los usuarios, existen aún muchas que aún no lo hacen, así como usuarios que no verifican que sus conexiones estén cifradas, lo cual se constituye en otro factor de riesgo, como veremos más adelante.

El uso de este tipo de redes o la falta de medidas de seguridad para su uso, facilita que un atacante dentro de dicha red pueda robar información que no haya sido cifrada, como se muestra a continuación:

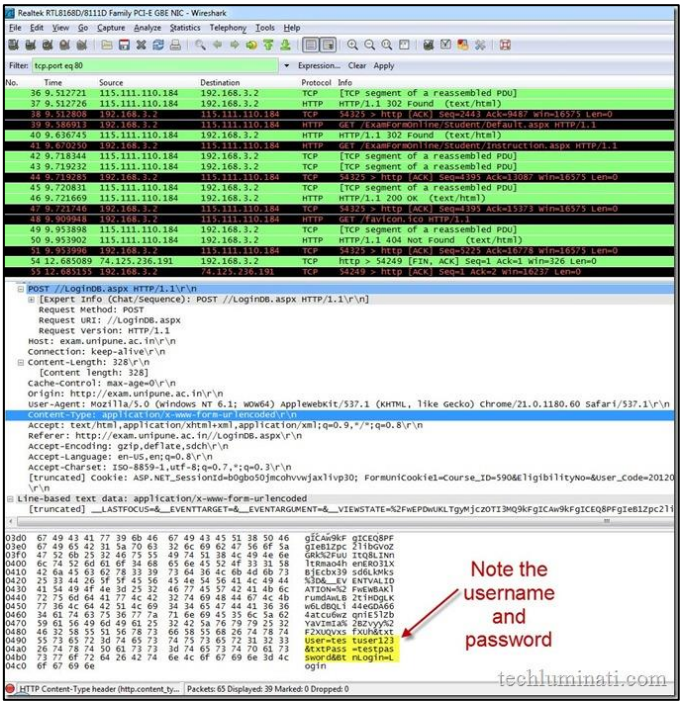

Figura 20 - Captura de información personal mediante el uso de Wireshark en una red pública (Fuente: http://techluminati.com/networking-and-security/student-of-university-of-pune-warning-your-personal-information-is-at-risk/)

8.4. DESCUIDO CON LAS CONTRASEÑAS

Las contraseñas son a los sistemas informáticos como las llaves a una cerradura física en una puerta de acceso a una instalación física, en tal virtud vale la pena detenerse un poco a evaluar un poco la seguridad de esta forma de autenticación. La comparación de una contraseña con la llave de una cerradura es útil para dimensionar la importancia de la misma, ya que sería interesante evaluar ¿qué cantidad de personas estaría dispuesta a utilizar una llave sin clave o combinación para acceder a la puerta de su casa? por ejemplo; o bien ¿quiénes dejarían la llave de la puerta pegada a la cerradura? Con el fin de facilitar su ubicación al momento de ser necesario su uso.

Pues bien, los ejemplos descritos anteriormente son un símil de lo que gran parte de las personas hacen hoy en día al momento de constituir una contraseña o durante su uso; es muy común encontrar contraseñas que son fácilmente predecibles, como lo indica uno de los rankings de las peores contraseñas.

RANK	PASSWORD	CHANGE FROM 2015
1	123456	Unchanged
2	password	Unchanged
3	12345	2 ↗
4	12345678	1 ↘
5	football	2 ↗
6	qwerty	2 ↘
7	1234567890	5 ↗
8	1234567	1 ↗
9	princess	12 ↗
10	1234	2 ↘
11	login	9 ↗
12	welcome	1 ↘
13	solo	10 ↗
14	abc123	1 ↘
15	admin	NEW
16	121212	NEW
17	flower	NEW
18	password	6 ↗
19	dragon	3 ↘
20	sunshine	NEW
21	master	4 ↘
22	hottie	NEW
23	loveme	NEW
24	zaq1zaq1	NEW
25	password1	NEW

Figura 21 - Ranking de las peores contraseñas del 2016
(Fuente: https://www.teamsid.com/worst-passwords-2016/)

El hacer uso de contraseñas tan predecibles como las que se exponen en la Figura 21, sería similar a utilizar llaves lisas o sin una combinación que dificulte establecer su diseño, como la que se muestra en la Figura 22, sería interesante realizar un conteo de las personas que hacen uso de una llave similar a esta para ingresar a su residencia, por ejemplo.

Figura 22 - Ejemplo de una llave sin combinación
(Fuente: https://www.assaabloy.cl/llave-alta-seguridad-sin-cifrar-yale/)

No obstante, hay personas que son conscientes de la importancia de una contraseña y al momento de estructurarlas utilizan métodos que las hacen más robustas, sin embargo descuidan otro aspecto importante en el uso de este método de autenticación y es la preservación secreta de la misma, dejándolas en sitios de fácil acceso de forma que se facilite su uso cuando sea requerido; ejemplo de esto sucede con la mayor parte de los enrutadores Wi-Fi que son entregados por la empresas proveedoras de servicio.

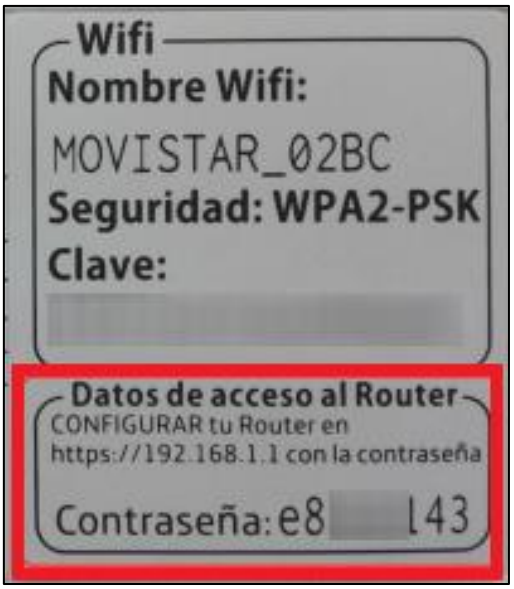

Figura 23 - Ejemplo de una contraseña pegada al dispositivo protegido (Fuente: https://comunidad.movistar.es/t5/Soporte-T%C3%A9cnico-Banda-Ancha/PROBLEMA-CONECTIVIDAD-PS4-Y-PSN-ROUTER-MITRASTAR/td-p/2702078)

Esta práctica sería similar a dejar colgada la llave de la puerta de la residencia de una persona colgada en la cerradura (como se muestra en la Figura 24), con el fin de facilitar su uso; nuevamente sería interesante calcular cuántas personas dejarían la llave pegada a la cerradura de sus casas. Al igual que sucede con la llave de una cerradura física, la cual perdería su razón de ser si se deja cerca a la cerradura que proteger, sucede con una contraseña que se deja pegada o cerca al dispositivo que proteger, esta también perdería su fundamento.

Figura 24 - Llave pegada a la cerradura (Fuente: https://es.dreamstime.com/imagen-de-archivo-libre-de-regal%C3%ADas-llaves-pegadas-en-una-cerradura-image36116686)

8.5. FALTA DE CIFRADO EN LA INFORMACIÓN

El cifrado de la información es un aspecto tan importante como complejo, ya que los sistemas de cifrado están orientados hacia la protección de la información sin importar lo que suceda con la misma; esto quiere decir que, si dicha información cayera en manos no autorizadas, la misma debería ser inútil para esas personas ya que no comprenderían el sentido de la misma. No obstante, la implementación de un sistema de cifrado es un asunto complejo, por lo que dicha práctica representa para los sistemas en términos de rendimiento, por lo cual es importante que los usuarios conozcan un poco del tema para aplicar los sistemas de cifrado que permiten desarrollar sus actividades de forma eficiente.

Es importante tener en cuenta que la no aplicación de estos métodos de protección podría impactar en la integridad y la confidencialidad de la información, ya que la misma podría ser accedida por personas no autorizadas que también podrían modificarla en el tránsito entre dispositivos dentro de una red.

8.6. FACILIDAD PARA EL ACCESO DE MALWARE

Este es uno de los aspectos más críticos en el manejo de la seguridad de una red, ya que son muchas las vías de acceso a través de las cuales se puede alojar un malware dentro de los sistemas que hacen parte de una red, entre las cuales se destacan las siguientes [10]:

- Sistemas de mensajería instantánea

- IRC (Internet Relay Chat)
- Dispositivos removibles
- Datos adjuntos
- Software legítimo empaquetado por un empleado descontento
- Errores de software de navegador y correo electrónico
- Archivos y carpetas compartidas
- Programas falsos
- Sitios maliciosos y software gratuito
- Descargar de archivos, juegos y otro tipo de archivos multimedia de sitios en Internet

Teniendo en cuenta las vías de acceso presentadas anteriormente, se puede determinar que el éxito de un malware depende en gran medida de la facilidad que de un usuario bien sea por acceder a links desconocidos que llegan a través de mensajes de texto de fuentes no confiables por ejemplo, el uso de dispositivos de almacenamiento removibles como USB's o discos duros extraíbles, los cuales en muchas ocasiones tienen orígenes desconocidos y pueden haberse visto comprometidos, la descarga de archivos adjuntos sin previa verificación, el uso de archivos y carpetas compartidas que pueden verse vulneradas por diferentes fuentes, las descargas de sitios maliciosos, etc. Lo anterior es una simple muestra de la gran cantidad de vectores de ataque que puede utilizar un malware para colarse dentro de una red y como el usuario final es en gran parte responsable del éxito del atacante.

Esta situación se hace más preocupante si se tiene en cuenta que la tendencia de crecimiento en la cantidad de malware existente es exponencial, lo que estadísticamente ayuda a aumentar las probabilidades de éxito de este tipo de amenazas.

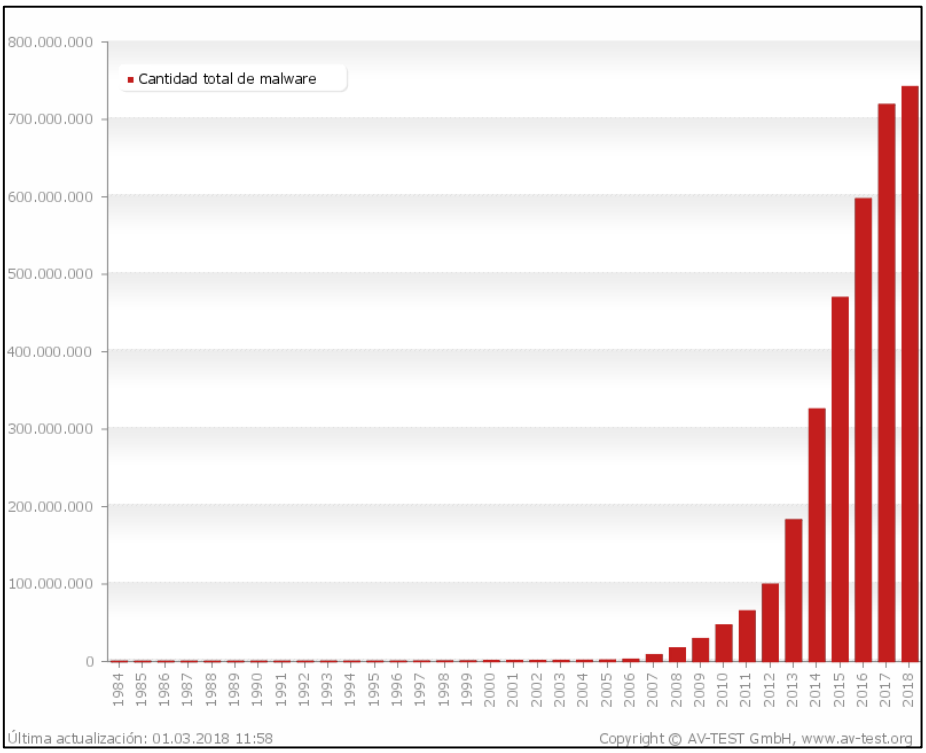

Figura 25 - Crecimiento anual en la cantida de malware existente (Fuente: https://www.av-test.org/es/estadisticas/malware/)

8.7. MANEJO INADECUADO DE METADATOS

Los metadatos se definen como datos acerca de los datos [2]; y cuando dichos datos no son manejados con precaución, le permitirían a un atacante obtener más información de la que sería necesario exponer en la red. Ejemplo de ello es que a través de los metadatos se puede llegar a conocer información tan valiosa como [11]:

- Nombres de empleados
- Nombres de usuarios de cuentas de sistemas informáticos
- Fechas de creación y modificación de archivos
- Coordenadas GPS en fotografías
- Versiones de software
- Rutas de directorios
- E-mails
- Direcciones MAC de tarjetas de red

- Direcciones IP
- Contraseñas

La mayor parte de esta información se encuentra pública en Internet y lo más probable es que la organización desconozca de su existencia; esta información le permitiría a un atacante establecer el mapa de red perfectamente estructurado [11]. Un ejemplo de la información expuesta de una organización que se puede obtener a través de metadatos se presenta a continuación.

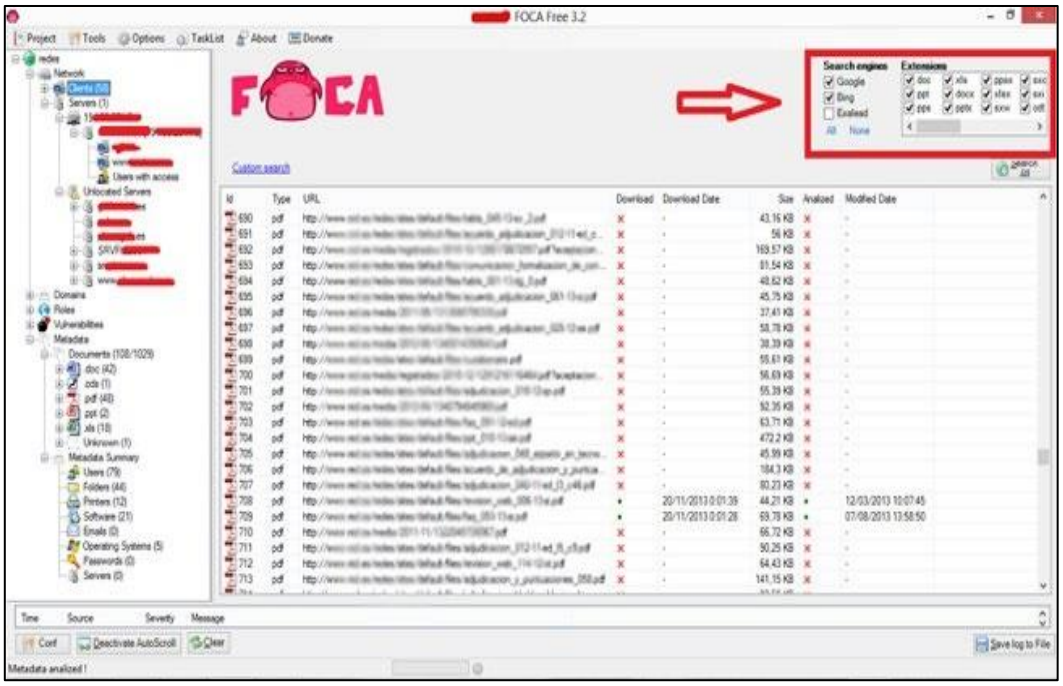

Figura 26 - Ejemplo de la información expuesta de una organización a través de metadatos (Fuente: https://www.incibe.es/protege-tu-empresa/blog/metadatos-webs-empresas)

8.8. USO DE SISTEMAS INFORMÁTICOS EN MODO "SUPERUSUARIO"

Aunque dentro de las organizaciones con políticas de seguridad robustas, a los usuarios generalmente se les asignan cuentas con privilegios restringidos, existen muchas entidades donde esta medida no se ha implementado por falta de sistemas que permitan su control o por simple descuido.

Para los diferentes sistemas operativos existe se configura un usuario que tiene todos los permisos necesarios para administrar dicho sistema; en Windows por ejemplo este usuario se conoce como "administrador" y el Linux se conoce como "root". El hecho es que cuando un usuario utiliza su sistema en modo "superusuario" le facilita el control total de su propio sistema a un atacante que tenga éxito en la explotación de alguna vulnerabilidad presente

dentro de dicho sistema, incluso facilitaría el control de otros sistemas conectados a su red, mediante la aplicación de técnicas de "pivoting".

Cuando un atacante compromete un sistema operativo mediante la explotación de una vulnerabilidad, generalmente adquiere los privilegios de la cuenta que está siendo utilizada en dicho momento, lo que le obligaría a aplicar otra técnica que se conoce como elevación de privilegios; sin embargo esta no sería necesaria si el usuario comprometido tienen privilegios de "administrador" o "root".

8.9. MANEJO INADECUADO DE PERMISOS OTORGADOS A APLICACIONES

En la actualidad es muy común encontrar aplicaciones que solicitan diferentes permisos dentro del sistema operativo dónde se van a alojar, es entonces importante que el usuario aprenda a identificar los permisos que debe otorgar según el tipo de aplicación que esté instalando en su dispositivo, ya que muchas de las aplicaciones que se encuentran disponibles hoy en día en el mercado, también son utilizadas para robar información confidencial de las personas.

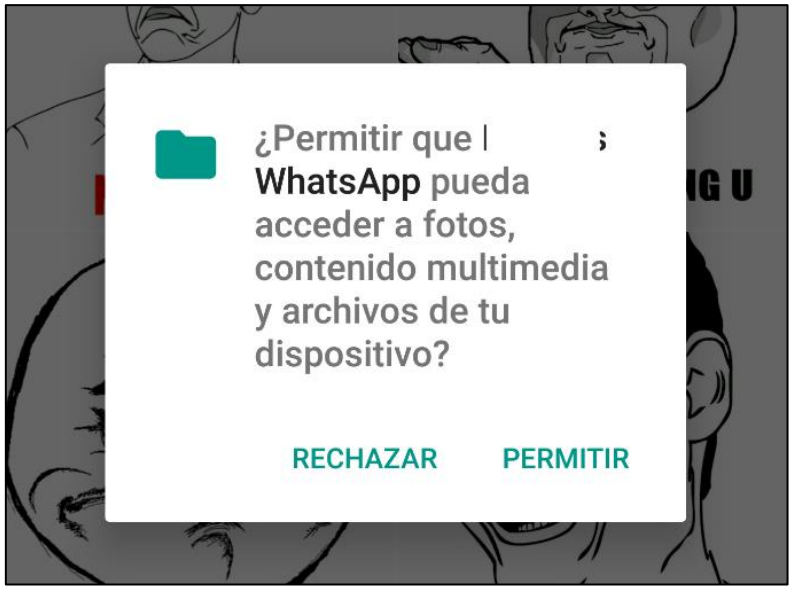

Figura 27 - Ejemplo de aplicación requieriendo permisos adicionales (Fuente: https://androidstudiofaqs.com/tutoriales/dar-permisos-a-aplicaciones-en-android-studio)

Como se muestra en la Figura 27, la mayor parte de las aplicaciones que instalamos en nuestros dispositivos requieren permisos adicionales para realizar acciones dentro de nuestros dispositivos, de ahí la importancia en saber identificar que tipo de permisos deberíamos autorizar, con el fin de evitar abrirle la puerta a atacantes que pueden aprovecharse de la necesidad del usuario para permear sus sitema.

9. PLAN DE SENSIBILIZACIÓN

Hasta este punto se ha identificado los principales orígenes de las amenazas que actualmente se encuentran latentes en el ciberespacio, las cuales están directamente vinculados con las malas prácticas desplegadas por la mayor parte de los usuarios de los sistemas TIC y que pueden llegar a generar un impacto negativo en la seguridad digital de las organizaciones.

Los principales factores de riesgo que dan paso a las amenazas cibernéticas, generados por comportamientos se listan a continuación:

- Uso inadecuado de las redes sociales
- Mal manejo de la política BYOD
- Conexiones a redes de poca confianza
- Descuido con las contraseñas
- Falta de cifrado en la información
- Facilidad para el acceso de malware
- Manejo inadecuado de metadatos
- Uso de sistemas informáticos en modo “superusuario”
- Manejo inadecuado de permisos otorgados a aplicaciones

Teniendo como punto de partida la identificación de los anteriores factores de riesgo, los cuales dan paso a las principales amenazas cibernéticas, identificadas y clasificadas anteriormente; a continuación, se procede a estructurar un plan de sensibilización que conduzca a mitigar las malas prácticas de los usuarios, las cuales muchas veces se presentan por desconocimiento de los riesgos cibernéticos.

9.1. CONSIDERACIONES PREVIAS

Para el diseño el presente plan, además de las amenazas y riesgos descritos en capítulos anteriores, se han tenido en cuenta los siguientes aspectos:

- La mayor parte de los usuarios de sistemas TIC’s dentro de las organizaciones no tiene un conocimiento tecnológico profundo que le permita entender la arquitectura de este tipo de sistemas y los protocolos que se encuentran implementados.

- El Usuario es el centro de los diferentes tipos de sistemas TIC, lo que hace que gran parte del éxito de un programa de ciberseguridad dependa de él, por lo que es indispensable sensibilizarlo y capacitarlo en temas relacionados con los riesgos cibernéticos.

- El desconocimiento generalizado, por parte de los usuarios de sistemas TIC, hace que sean fácilmente vulnerables, ya que podrían caer en cualquiera de los diferentes tipos de estrategias que utilizan los atacantes para permear la seguridad de los sistemas informáticos; ya que, como dijo Ariel Torres: "Es más fácil hackear a una persona que a una máquina"[4].

- El diseño e implementación de un plan de sensibilización en temas relacionados con amenazas cibernéticas debe estar orientado a disminuir la superficie de ataque generada por el uso de sistemas TIC.

- El éxito de un plan de sensibilización debe ser medible a través de los resultados de su implementación, los cuales deben ser medibles mediante la disminución de incidentes cibernéticos.

- El plan de sensibilización deberá estar sometido a un proceso de actualización y mejora continua, el cual debe estar sustentado en la evolución de las amenazas cibernéticas y los resultados obtenidos mediante la implementación del plan.

- El diseño del plan deberá estar basado en el nuevo paradigma de la ciberseguridad, denominado "presunción de la brecha", mediante el cual se asume que el atacante se encuentra dentro del perímetro de seguridad de las redes informáticas de una organización.

9.2. OBJETIVOS DEL PLAN

A continuación, se presentan los objetivos bajo los cuales se estructura el plan de sensibilización propuesto.

9.2.1. General

Disminuir el impacto generado por los principales factores de riesgo generados por el desconocimiento generalizado, respecto al ciberespacio y las amenazas inherentes al mismo, reflejado por la mayor parte de los usuarios de los sistemas informáticos.

9.2.2. Específicos

[4] Tomada de: https://www.infobae.com/tecno/2017/09/16/es-mas-facil-hackear-a-una-persona-que-a-una-maquina/

- Determinar las estrategias bajo las cuales se puede diseñar e implementar un programa de sensibilización sobre riesgos y amenazas cibernéticas, que pueda ser aplicable a la mayor parte de organizaciones.

- Diseñar espacios que permitan informar a los usuarios sobre los riesgos que se encuentran latentes en el ciberespacio, así como las medidas que se deben tomar para hacer frente a dichas amenazas.

- Diseñar espacios que conduzcan a generar confianza entre el personal encargado de la ciberseguridad de la organización y los usuarios de los sistemas conectados a la red.

- Generar campañas a través de las cuales se incentive a los usuarios de la organización a tomar medidas que conduzcan a hacer más seguro el uso del ciberespacio.

- Establecer los medios de difusión que se pueden utilizar para el desarrollo del plan de sensibilización.

- Describir las diferentes actividades que harían parte del plan de sensibilización.

- Diseñar parámetros que permitan medir el nivel de eficiencia del plan durante su implementación.

9.3. CONTENIDO TEMÁTICO DEL PLAN

Teniendo en cuenta los factores de riesgo identificados previamente, se considera necesario que a través del plan de aborden los siguientes ejes temáticos:

9.3.1. Descripción del ciberespacio

A través del desarrollo de este eje el usuario deberá conocer de forma superficial la arquitectura del ciberespacio y cómo funciona este, de forma que comprenda cuáles de las características del mismo, dan origen a los riesgos y amenazas que se encuentran latentes en la actualidad dentro de este medio.

9.3.2. Riesgos y amenazas en el ciberespacio

Este eje temático debe estar orientado a que el usuario esté en la capacidad de identificar los riesgos y amenazas en el ciberespacio, ya que gran parte de los incidentes informáticos dentro de una organización, se presentan porque un usuario cae en una trampa diseñada por un atacante.

9.3.3. Medios de protección para el uso de Internet

El desarrollo de este eje debe contribuir a que el usuario identifique las principales medidas de seguridad que debe adoptar para el uso seguro de Internet, no sólo cuando se encuentre dentro de la red de la organización sino en todo momento, con el fin de evitar brechas de seguridad que impacten de forma negativa dentro de la organización.

9.3.4. Seguridad de dispositivos móviles

Teniendo en cuenta que la mayor parte de los usuarios en la actualidad acceden a Internet a través de dispositivos móviles, como se evidencia en la Figura 28, se hace necesario que los usuarios de la organización donde se desarrolle el presente plan, conozcan las medidas mínimas que deberían implementar en sus dispositivos con el fin de disminuir los principales riesgos que se generan por el uso de los mismos sin observar unos hábitos adecuados que conlleven a mitigar los riesgos cibernéticos.

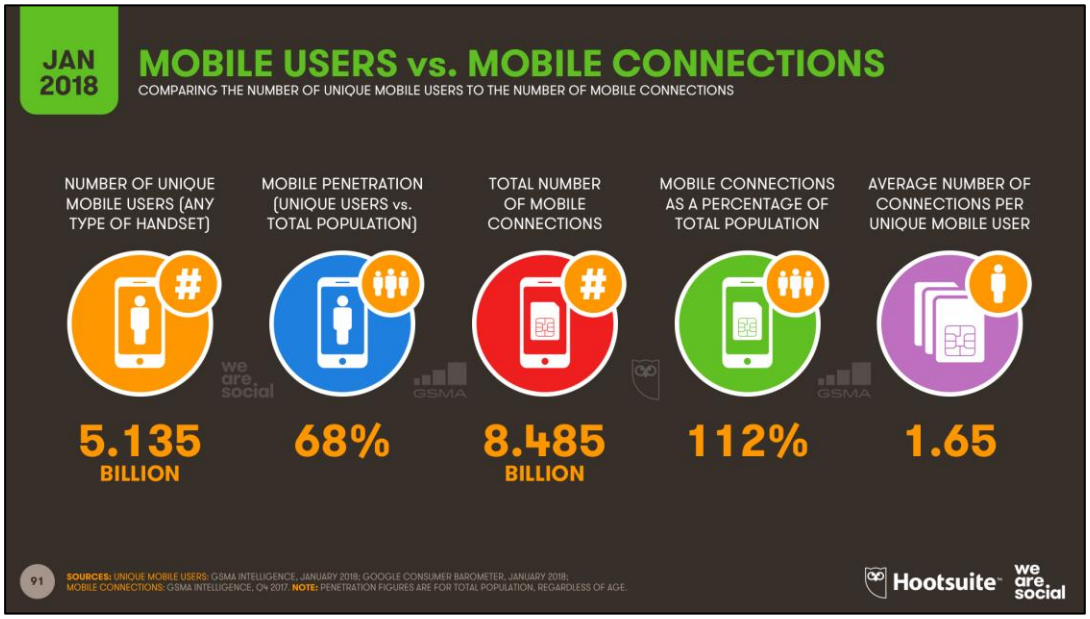

Figura 28 - Uso de dispositivos móviles (Fuente: https://wearesocial-net.s3.amazonaws.com/wp-content/uploads/2018/01/DIGITAL-IN-2018-005-MOBILE-USERS-vs-MOBILE-CONNECTIONS-V1.00-.png)

9.3.5. Estrategias para protección de los datos

Otro de los ejes temáticos importantes que se deben considerar dentro del presente plan es sensibilización sobre la importancia de proteger los datos que almenamos y/o trasmitimos a través de los sistemas TIC, con el fin de evitar que dicha información caiga en manos no autorizadas o que la misma pueda ser alterada durante el tránsito entre diferentes sistemas interconectados.

9.3.6. Contraseñas seguras

Cómo se mostró en uno de los capítulos anteriores, uno de los errores más comunes que reflejan gran parte de los usuarios se presenta en el establecimiento y control de las contraseñas que utilizan para autenticarse en los diferentes servicios y sistemas; por lo anterior, se considera pertinente enfocar uno de los ejes temáticos hacia la sensibilización sobre la importancia de establecer contraseñas que reflejen condiciones de seguridad eficientes, así como la administración de las mismas, de forma que se evite que estas caigan en manos de personas no autorizadas.

9.3.7. Endurecimiento de la seguridad

Otro aspecto temático importante que se deberá incluir dentro del plan de sensibilización es el conocimiento sobre acciones que puedan realizar los usuarios dentro de los sistemas que utilizan, con el fin de endurecer la seguridad de los sistemas, dificultando de esta forma las técnicas que utilizan los atacantes.

9.4. ESTRATEGIAS

El plan deberá ser desarrollado bajo las siguientes estrategias.

9.4.1. Explotación de los beneficios de las redes sociales

Como se mencionó en capítulos anteriores, uno de los factores de riesgo más críticos se genera por el mal manejo de la información que la mayor parte de los usuarios hace pública a través de las diferentes redes sociales; esto se debe en gran medida al creciente uso de este tipo de plataformas, como se evidencia a continuación.

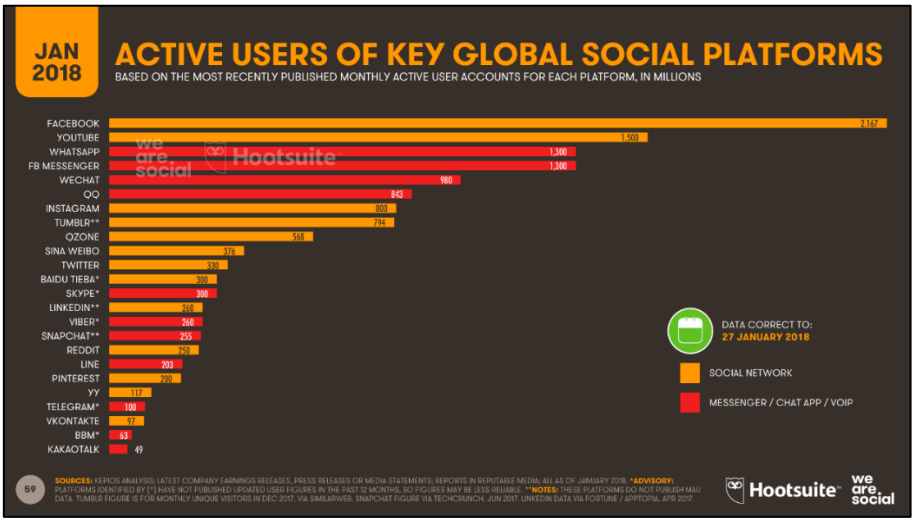

Figura 29 - Cantidad de usuarios activos en las principales redes sociales (Fuente: https://wearesocial-net.s3.amazonaws.com/wp-content/uploads/2018/01/DIGITAL-IN-2018-012-SOCIAL-MEDIA-PLATFORM-RANKING-V1.00.png)

Por lo anterior, se considera relevante hacer uso de este tipo de herramientas como medio de difusión de información, dentro de las actividades que se contemplen dentro del desarrollo del presente plan, de forma que un factor de riesgo se convierta en una herramienta que permita impactar permanentemente la conciencia de los usuarios de los sistemas TIC de una organización.

Para el desarrollo de esta estrategia es necesario que las organizaciones se vinculen con las diferentes redes sociales, especialmente con aquellas que son más populares entre los miembros de la organización donde se implemente el presente plan. Para ello se requiere inicialmente adelantar encuestas internas que permitan identificar aquellas plataformas que sean más utilizadas.

Al tener identificadas las principales redes sociales utilizadas dentro de la organización donde se pretenda implementar el presente plan de sensibilización se diseñará una campaña informativa, mediante el despliegue de panfletos de alerta y concienciación sobre amenazas cibernéticas de forma permanente.

9.4.2. Generar necesidad de conocimiento a los usuarios

Los temas tecnológicos son poco atractivos para aquellas personas que no tienen un vínculo estrecho con las TIC's, a pesar de esto la penetración tecnológica en el mundo es un aspecto que crece constantemente (como se aprecia en la Figura 30); las cifras demuestran que el vínculo hombre – tecnología es una característica del mundo actual, por lo cual es importante que los usuarios conozcan un poco más sobre los sistemas que utilizan, sobre todo si a través de los mismos se transmite o almacena información que pueda ser utilizada en contra de ellos o de las instituciones a las cuales pertenecen.

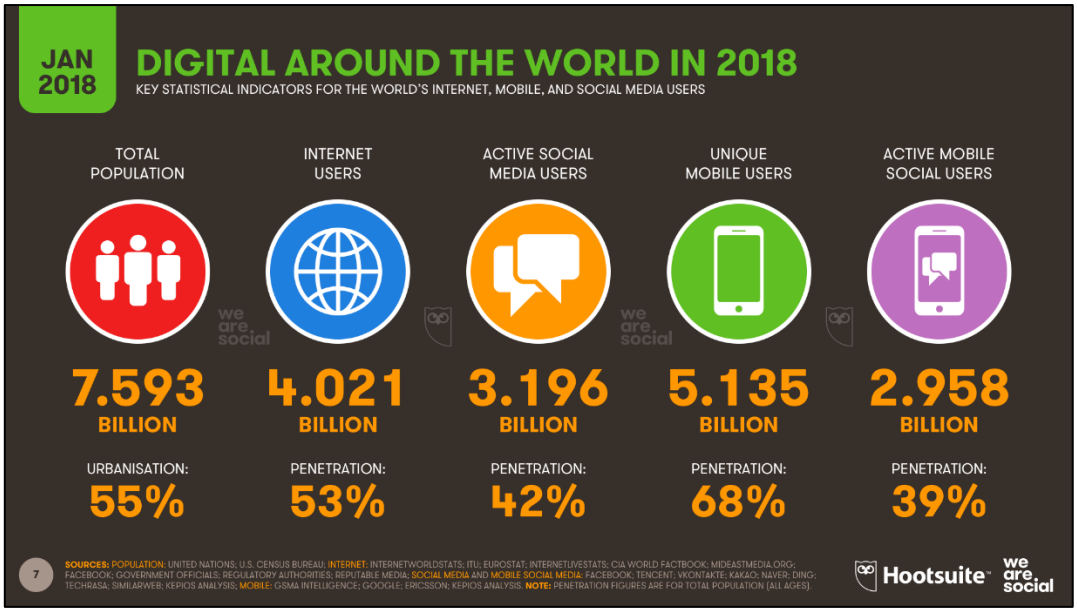

Figura 30 - Pentración tecnológica en el mundo (Fuente: https://wearesocial-net.s3.amazonaws.com/wp-content/uploads/2018/01/DIGITAL-IN-2018-001-GLOBAL-OVERVIEW-V1.00.png)

Por lo anterior, una de las estrategias fundamentales para el desarrollo del presente plan, debe estar enfocada en generar la necesidad de que el usuario se interese por buscar y comprender en mayor profundidad la información relacionada con las amenazas cibernéticas emergentes.

Para ello se deberá identificar el tipo de sistemas de mayor acogida dentro de la organización donde se desee implementar el presente plan, dicha identificación debe permitir caracterizar principalmente los siguientes aspectos:

- El mayor porcentaje de dispositivos utilizados por los usuarios de la organización, computadores, tablets, teléfonos móviles, etc.

- El tipo de sistemas operativos preferidos por los usuarios de la organización, Windows, MacOS, Linux, Android, etc.

- El tipo de aplicaciones que más se utilizan en los diferentes dispositivos, navegadores web, redes sociales, software de ofimática, etc.

Esta información deberá ser obtenida mediante encuestas que se realicen al interior de la organización y con base en los resultados obtenidos, se podrán establecer ejes temáticos principales para la difusión constante de información relacionada con amenazas y vulnerabilidades relevantes que puedan afectar los sistemas de interés para los usuarios de la entidad donde se desarrolle el presente plan.

9.4.3. Utilización de un lenguaje llamativo

El manejo de sistemas relacionados con Tecnologías de la Información y las Comunicaciones implica en muchas ocasiones el uso de un lenguaje que algunas veces tiende a ser muy técnico para la mayor parte de los usuarios, por lo que se considera importante que para el desarrollo de las actividades propias del presente plan se utilice un lenguaje que sea llamativo para la mayor parte de las personas sin importar su nivel de conocimiento técnico.

El desarrollo de esta estrategia dentro del plan puede llegar a ser un aspecto complicado, ya que para explicar la forma en que se comportan las amenazas cibernéticas, en muchas ocasiones es necesario acudir a expresiones que sólo cobran sentido mediante el uso de términos técnicos; por lo anterior es importante que al momento de diseñar las actividades y contenido propio del plan se contemple dentro del equipo la participación de personas con conocimiento en publicidad, de forma que sirvan de apoyo para impactar de mejor manera a los usuarios de los sistemas TIC dentro de la organización.

9.5. MEDIOS

Para el desarrollo del presente plan, se ha considerado que se deberían utilizar los siguientes medios de difusión de información, los cuales están disponibles en la mayoría de las organizaciones de hoy en día.

9.5.1. Redes sociales

Como se mencionó anteriormente, una de las estrategias planteadas para el desarrollo del presente plan es el uso de las redes sociales más utilizadas por los miembros de la organización blanco del presente plan, con el fin de difundir de forma permanente información que sensibilice sobre la importancia de observar y acoger las medidas de seguridad necesarias para garantizar la ciberseguridad de los propios usuarios y por ende la de la entidad a la cual pertenecen.

El objetivo que se pretende alcanzar con el uso de redes sociales, dentro del desarrollo del presente plan, es lograr que las personas interactúen permanentemente con información relacionada con los riesgos latentes en el ciberespacio y que compartan sus opiniones sobre las malas prácticas, relacionadas con el uso de sistemas TIC's, que se logren identificar y difundir.

Lo anterior permitirá impactar positivamente en los hábitos de los usuarios de sistemas TIC pertenecientes a la organización, además que contribuirá a mitigar uno de los factores de riesgo más relevantes, el uso inadecuado de las redes sociales; además que le permitirá a la organización interactuar con los usuarios de la compañía a través de medios cibernéticos llamativos.

Para que estas plataformas sean eficientes para alcanzar los objetivos propuestos por la campaña, es necesario que se logre que los usuarios de los sistemas TIC de la organización sigan los perfiles propios de la entidad, por lo cual dichas plataformas no sólo pueden ser utilizadas para el desarrollo de la presente campaña sino que además deben difundir información que sea interesante para los usuarios, bien sea sobre las actividades propias de la institución o sobre temas de interés general, de forma que los mismos se conviertan en la ventana de atracción hacia la información que se pretende difundir a través del presente plan.

Por lo anterior el uso de las redes sociales de la organización se haría de la siguiente forma:

1. Establecer un portafolio de temas de interés general.

2. Establecer espacios a través de los cuales se difunda información relacionada con los temas establecidos.

3. Establecer periodos de actualización de dichos espacios.

4. Entre los espacios establecidos y previa verificación de la aceptación entre los diferentes usuarios, se dispondrá de un espacio adicional para la difusión de información relacionada con dos ejes principales:

    - Campaña de sensibilización, a través de la cual se deberá buscar que los usuarios sean conscientes de la necesidad de tomar medidas permanentes tendientes a garantizar su ciberseguridad y por ende la de la organización a la que pertenecen.

    - Sistema de alertas, a través del cual se difunda información sobre nuevas vulnerabilidades o técnicas de ataques cibernéticos que puedan afectar a los usuarios.

Para el uso de este tipo de medios también se deberá considerar una de las estrategias descritas anteriormente, el uso de un lenguaje llamativo; además se deberá considerar el uso de información que sea corta y que busque generar un alto impacto.

9.5.2. Correos electrónicos

Otro medio importante que permite realizar la difusión de información inherente al presente plan, es el correo electrónico institucional, mediante el cual se pueden generar un sistema de boletines informativos y alertas, en los cuales se podría profundizar un poco más la información, incluyendo enlaces que generen curiosidad en los usuarios, de forma que se les lleve a conocer más información sobre las diferentes amenazas a las que se encuentran expuestos.

De igual forma el servicio de correo electrónico Institucional puede ser utilizado como medio demostrativo de lo que un atacante puede hacer, enviando señuelos que conlleven a demostrar lo que les sucede a los usuarios que acceden a información enviada por personas o entidades desconocidas.

9.5.3. Carteleras informativas de la organización

Dentro de la mayor parte de las organizaciones, hoy en día se encuentran diferentes tipos de carteleras informativas donde se plasma información de interés general para el persona de la entidad; este medio de comunicación puede ser también utilizado como medio de difusión de mensajes muy cortos pero llamativos mediante los cuales se genere permanentemente conciencia sobre la importancia de que el usuario fortalezca sus medidas de seguridad de forma continua.

9.5.4. Página Intranet de la Organización

Este también es otro medio que pude ser mu útil en el desarrollo del presente plan, toda vez que as través de este tipo de plataformas, los usuarios acceden permanentemente a los servicios y sistemas en red con los que cuenta la organización, por lo que al igual que otro tipo de plataformas, esta permitiría la difusión masiva entre los diferentes usuarios de la

organización, principalmente hacia aquellos que utilizan los sistemas informáticos de la misma.

9.5.5. Charlas informativas

Dentro del desarrollo del presente plan es relevante que se contemplen espacios de información, sensibilización y capacitación, donde se abarquen los diferentes ejes temáticos planteados al inicio del presente capítulo; la importancia de este medio es la posibilidad de interacción bidireccional entre el grupo encargado de la implementación del presente plan, lo cual permitiría la resolución de dudas respecto a la temática tratada así como la percepción del nivel de aceptación del desarrollo del plan por parte del blanco audiencia.

Dentro de estas charlas también es importante que se den a conocer y se capacite al personal de la organización en la importancia de acatar las Políticas, Normas y Procedimientos de Ciberseguridad que se hayan estructurado para la organización, por lo cual se debe propender por la participación masiva de los miembros de la organización.

9.5.6. Otros medios

Además de los medios descritos anteriormente, se debería acudir a cualquier espacio que permita entregar de forma permanente a los usuarios, información que genere conciencia sobre el riesgo latente en el ciberespacio y las acciones que se deben adelantar para mitigarlos. Algunos de esos espacios podrían ser:

- Volantes que sean repartidos entre los diferentes usuarios
- Pendones publicitarios que se ubiquen en las zonas de alto tráfico dentro de la organización
- Folletos y plegables
- Protectores de pantalla
- Calendarios
- Mugs publicitarios

9.6. ACTIVIDADES

9.6.1. Primera parte: sensibilización sobre el ciberespacio

La primera parte del plan debe basarse en el desarrollo de un programa de capacitación que esté orientado a entregar la información básica que le permita a los usuarios de los sistemas TIC de la organización comprender la arquitectura del ciberespacio así como la forma en que los sistemas se comunican entre sí y de forma básica como se comportan los protocolos utilizados para el intercambio de información.

De igual forma, en esta primera parte del desarrollo del plan se deberá entregar información sobre las principales amenazas cibernéticas a las cuales se encuentran expuestos los usuarios de cualquier sistema TIC y la forma como estas amenazas podrían afectar la seguridad individual de cada usuario llegando a impactar incluso en la seguridad digital de la organización a la cual pertenecen.

El objetivo del desarrollo de la primera parte del plan deberá estar orientado a nivelar los conocimientos básicos en cuanto al ciberespacio y los riesgos asociados a su uso, de forma que los usuarios de las redes de la organización cuenten con las herramientas cognitivas que les permitan identificar los riesgos durante el uso de sistemas TIC.

9.6.2. Segunda parte: difusión permanente información sobre amenazas

Habiendo establecido un nivel de conocimientos básicos sobre el ciberespacio y los riesgos implícitos durante su uso, se deberá proceder a mantener de forma permanente campañas informativas relacionadas con las nuevas amenazas cibernéticas, las nuevas técnicas utilizadas por los atacantes y las acciones que deberían adelantar los usuarios para mitigar los riesgos.

Es también necesario que se mantenga un esfuerzo por utilizar medios audiovisuales de impacto que estén generando conciencia sobre la importancia de observar y mantener las medidas de seguridad durante el uso de sistemas TIC, de forma que el usuario se sienta vinculado e importante para el proceso de ciberseguridad de la organización.

Dichas campañas se podrían lanzar mediante el uso de mensajes similares a los que se presentan a continuación:

Figura 31 - Ejemplo de imagenes que se puede utilizar en folletos y/o pendones (Fuente: Comité de Seguridad de la Información)

Como se mencionó anteriormente es también muy importante que, a través de los medios especificados para el desarrollo del presente plan y con fundamento en las estrategias planteadas al inicio del presente capítulo, se diseñe un sistema que permita mantener la alerta por parte de los usuarios sobre nuevas técnicas, vulnerabilidades o amenazas que se identifiquen en el ciberespacio, así como las respectivas recomendaciones que conlleven a mitigar los riesgos que estas situaciones generarían tanto para los usuarios como para la organización.

Es importante tener en cuenta que en este tipo de alertas se utilice un leguaje poco técnico, de formas que la mayor parte de las personas pueda comprender fácilmente el riesgo de las situaciones sobre las cuales se pretende alertar. Un ejemplo de la forma como se podría difundir este tipo de información se presenta a continuación:

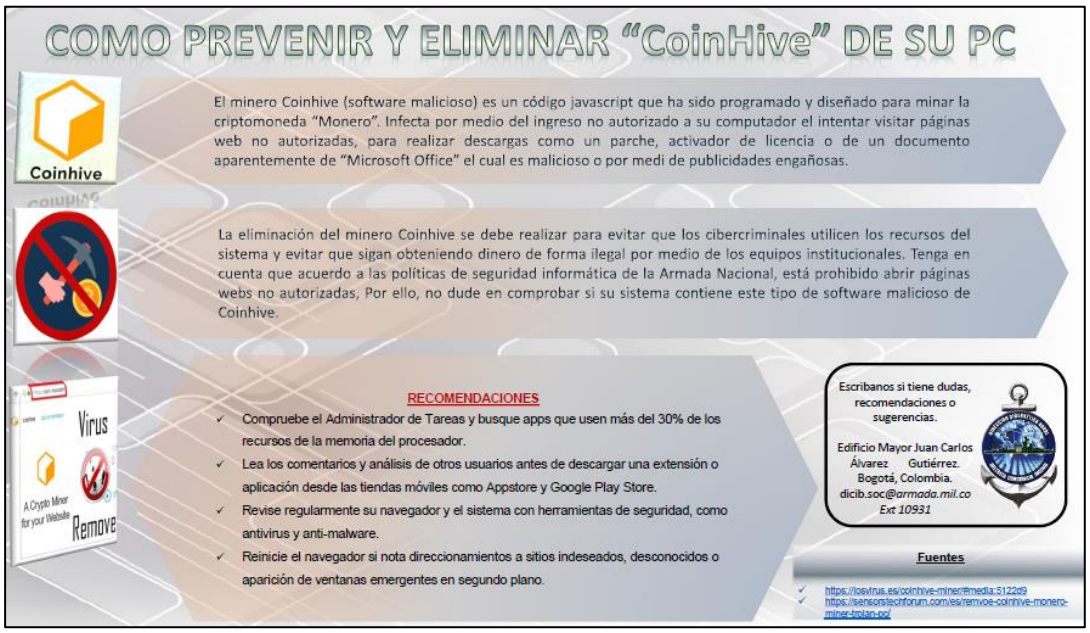

Figura 32 - Ejemplo de alerta sobre riesgos cibernéticos (Fuente: Sistema de alertas cibernéticas de la Armada Nacional de la República de Colombia)

Como se evidencia en la Figura 32, este tipo de alertas debe contener información muy puntual sobre la situación que genera riesgo y unas recomendaciones puntuales para mitigarlo, de igual forma debe contener enlaces que permitan ampliar información al respecto para aquellos usuarios que les haya despertado curiosidad la situación informada.

9.6.3.Tercera parte: evaluación y mejora y continua

El desarrollo de la tercera parte del plan se constituiría en uno de los ejes principales para el éxito del mismo y contribuiría a mejorar de forma permanente los resultados que se alcancen mediante el mismo; la evaluación periódica del plan permitirá identificar debilidades y fortalezas del mismo, de forma que se puedan planear ajustes que conduzcan a la mejora continua.
Como proceso de evaluación y mejora para el presente plan se hace necesario adelantar las siguientes actividades:

9.6.3.1. Levantamiento de información preliminar

Antes de desarrollar el presente plan, se deberá hacer un levantamiento sobre la información estadística que permita determinar la situación actual de la organización, a través de dicha información se deberán establecer los siguientes aspectos:

- Cantidad de incidentes informáticos que está enfrentando la organización periódicamente (Diariamente, semanalmente, mensualmente y anualmente).

- Estadísticas de los sistemas más afectados dentro de la organización (Computadores, dispositivos portátiles, servidores, etc.).

- Estimación de pérdidas económicas generadas por incidentes cibernéticos.

- Estimación porcentual de los incidentes que pudieron haber sido generados por fallas humanas.

Esta información permitirá establecer la situación preliminar sobre los incidentes que se estarían generando dentro de la organización por fallas humanas y el impacto que estaría generando para los sistemas informáticos, así como los costos que le habría implicado a la entidad esta situación. El resultado de esta primera actividad permitirá establecer el nivel de comparación base paras medir la eficiencia durante el desarrollo del plan.

9.6.3.2. Establecer periodos de evaluación

Teniendo en cuenta la información recopilada en el paso anterior, se deberá establecer la periodicidad con la cual se evaluará el desarrollo del plan de sensibilización, esto se determinará con base en la cantidad eventos que venga enfrentando en la organización; esto quiere decir que si la organización, por el tamaño de su infraestructura informática y su nivel de riesgo cibernético, viene enfrentando una cantidad considerable de incidentes en cortos periodos de tiempo, se deberá disminuir la periodicidad de evaluación; sin embargo, si por el contrario la entidad no enfrenta una cantidad considerable de eventos, la evaluación se deberá realizar en espacio de tiempo más amplios de forma que los resultados sean fácilmente apreciables.

La determinación del periodo es un aspecto importante dentro del proceso de evaluación, ya que permitirá que esta parte del tiempo sea eficiente a cuanto a la medición y análisis de resultados.

9.6.3.3. Establecer las fuentes de información

Es importante determinar cuales serán las fuentes de información que se tomarán como base para el desarrollo del proceso evaluativo, dentro de las mismas se deberá considerar las fuentes que se utilizaron para levantar la información preliminar, no obstante es relevante que se tengan en cuenta fuentes adicionales, tales como: encuestas, comentarios en redes sociales, interacciones durante charlas, etc.

9.6.3.4. Análisis de resultados

El éxito del plan de sensibilización se basará en la disminución permanente de incidentes de seguridad que se presenten dentro de las redes cibernéticas de la organización, por lo cual un eje de resultados relevante se sustenta en la cantidad de incidentes cibernéticos que se presenten después de iniciar el desarrollo del presente plan; de igual forma es importante

analizar la aceptación de los métodos y medios a través de los cuales se difunde la información, de forma que se conduzca a mejorar los resultados permanentemente.

9.6.3.5. Diseño de estrategias de mejora

Con base en el análisis de resultados se deberán diseñar estrategias de mejora que permitan mejorar los resultados que se obtengan con el desarrollo del presente plan, dichos planes deberán ser sometidos a la toma de decisiones por parte de la junta directiva (o quienes hagan sus veces) de la organización.

10. MEDICIÓN EXPERIMENTAL

A continuación, se plantea un procedimiento experimental que permitiría medir de forma más acertada el impacto después de la implementación del plan propuesto mediante el presente proyecto.

10.1. CONCEPTO

Ante el problema planteado al inicio del proyecto, se ha determinado que el concepto debe estar orientado a fortalecer la parte educativa del personal de usuarios de sistemas TIC dentro de las diferentes organizaciones, para ello es necesario diseñar y desarrollar inicialmente programas de capacitación que estén orientados a nivelar los conocimientos básicos del personal relacionados con el uso del ciberespacio y las amenazas inherentes, posteriormente se deberá hacer lo mismo con programas de sensibilización y entrenamiento permanente de forma que se conlleve a mantener a los usuarios actualizados en temas relacionados con las nuevas vulnerabilidades, amenazas y factores de riesgo, así como las acciones que debe desplegar el usuario para disminuir la posibilidad de ser víctimas de ataques cibernéticos.

Lo anterior se sustenta en la necesidad de mitigar los riesgos generados por el factor humano, es decir con el desarrollo de un plan de sensibilización que permita entre otros, la disminución permanente de incidentes de seguridad que se presenten dentro de las redes cibernéticas de la organización, así mismo es importante analizar la aceptación de los métodos y medios a través de los cuales se difunde la información, de forma que se conduzca a mejorar los resultados permanentemente.

Como se mencionó anteriormente, para garantizar el éxito del plan, se requiere que previamente se realicen actividades dentro de las que se destaca el levantamiento de información estadística que permita determinar la situación previa de la organización, identificando aspectos como la cantidad de incidentes informáticos, las cuales la organización viene generando periódicamente, en algunos casos se puede determinar que cuando no se esté evidenciando que existan datos estadísticos, al respecto podría caer una falsa sensación de seguridad y entender que no pasa nada o no hay incidentes cibernéticos, esto se da porque en algunos casos efectivamente el personal de la organización no sabe cuáles son los mecanismos para poder reportar incidentes, y el otro riesgos es por las consecuencias o el temor de reportar incidentes o eventos cibernéticos que ocurra, por lo cual el escenario debería evidenciarse al desarrollar este tipo de actividades previas al ejecutar el plan.

Así mismo es necesario tener información que permita estudiar el estado de la infraestructura tecnológica que soporta los sistemas de información; de igual forma es necesario cuantificar o tener unos datos que permitan estimar las pérdidas económicas ocasionadas por incidentes cibernéticos y finalmente es importante contar con la información y los métodos que permitan estimar el porcentaje de los incidentes cuya generación se puede haber presentado por fallas humanas.

La propuesta entonces es experimentar enfocando el esfuerzo sobre dos vectores principales orientados a la capacitación y el segundo a la sensibilización entrenamiento permanente relacionado con las técnicas y métodos para identificar y afrontar las amenazas a las cuales puedan estar expuestos los funcionarios de la organización, es decir el establecimiento de campañas informativas que le permitan al usuario lograr tener un conocimiento que le permita afrontar sobre los riesgos a los cuales se ve inmerso cuando hace uso de la tecnología.

Las campañas se soportarán sobre los diferentes medios de difusión informativa disponibles dentro de gran parte de las organizaciones, como son el apoyo de las redes sociales, volantes, pendones, folletos y plegables, calendarios, charlas informativos entre otros; lo más importante el usuario se sienta vinculado e importante para el proceso de ciberseguridad de la organización.

10.2. HIPOTESIS INICIAL

Otra manera para definir el problema, lo realizaremos haciendo uso de la selección de propuestas o hipótesis, buscando siempre un mayor conocimiento, se establecerán las proposiciones de forma organizada determinado las siguientes actividades:

10.3. COMPROMISO Y LA VISIÓN PERSONAL

El compromiso es la base para un proceso de aprendizaje, consideramos que no hay nada que sustituya el verdadero compromiso y a la visión personal. Por ello creemos que se debe creer en algo que importe personalmente. Si los funcionarios de una organización no se comprometen, no se puede sostener un proceso de aprendizaje significativo que le permita tener un conocimiento para finalmente obtener unos hábitos, para este caso el afrontar unos riesgos en los cuales estarían expuestos al hacer uso del ciberespacio.

10.4. ENTRENAMIENTO

En las organizaciones es la primera fase de cualquier proceso de capacitación e involucra no solamente un aprendizaje de información para el funcionario de la organización, si no también cambios en la conducta de este que contribuyen al logro de las metas individuales y organizacionales, es esencial que los procesos de entrenamiento se evalúen teniendo en cuenta su relevancia y pertinencia para el logro de los objetivos organizacionales.

10.5. FORMACION

La formación es el proceso resultante del conjunto de actividades destinadas a desarrollar en los funcionarios de la organización las habilidades aptitudes y actitudes que la misma necesitará en el futuro para hacer frente a las amenazas cibernéticas.

La formación organizacional no tendrá resultados a menos que esté vinculada con los objetivos en la organización. Un programa de formación bien diseñado surge objetivos

estratégicos. Un programa mal diseñado será aquel no tendrá relación alguna con estos objetivos o lo que es peor, que no loes entienda correctamente.

Como se informó anteriormente el plan de sensibilización va a permitir que los funcionarios de la organización posean unas bases de las cuales tiene un fundamento basados en estos tres grandes principios de una forma integrada y organizada.

10.6. PLANTEAMIENTO DEL EXPERIMENTO

Para el experimento se propone dos (2) tipos de ataque que podría generar resultados que permitan visualizar que lo efectivo del plan de sensibilización que se propone, estos son :

10.7. ATAQUE PHISING

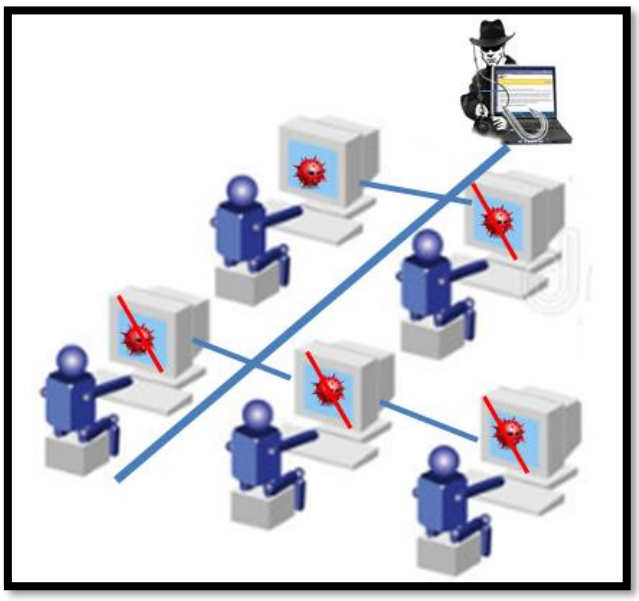

Figura 33 - Arquitectura de un esquema donde los funcionarios son afectados por un ataque phising (Fuente: Diseño Propio)

Debido a este ataque podemos establecer como medición las siguientes variables

1. Porcentaje de usuarios afectados ante el incidente cibernético.
2. Número de horas, sin servicio
3. Cantidad de aplicaciones sin acceder.

10.8. ATAQUE DE INGENIERIA SOCIAL

Figura 34 - Arquitectura de un esquema donde los funcionarios son afectados por un ataque de Ingeniería Social (Fuente: Adaptación / https://www.pabloyglesias.com/ingenieria-social-profesionalizada/)

Este otro tipo de ataque que tiene una frecuencia alta es la de ingeniería social, se pueden establecer la medición con las siguientes variables, así:

1. Numero de intentos para extraer información,
2. Cantidad de incidentes generados por ingeniería social.
3. Numero funcionarios afectados por la ingeniera social.

10.9. RESULTADOS POSTERIORES AL PLAN

Los resultados esperados permitirían demostrar que una vez adoptado el plan de sensibilización, los funcionarios adoptan una mejor actitud, frente a amenazas cibernéticas como el phishing, por ejemplo, generando mejores hábitos y protegiéndose así mismos contribuirían a la protección de la infraestructura tecnológica de la organización a la cual pertenecen.

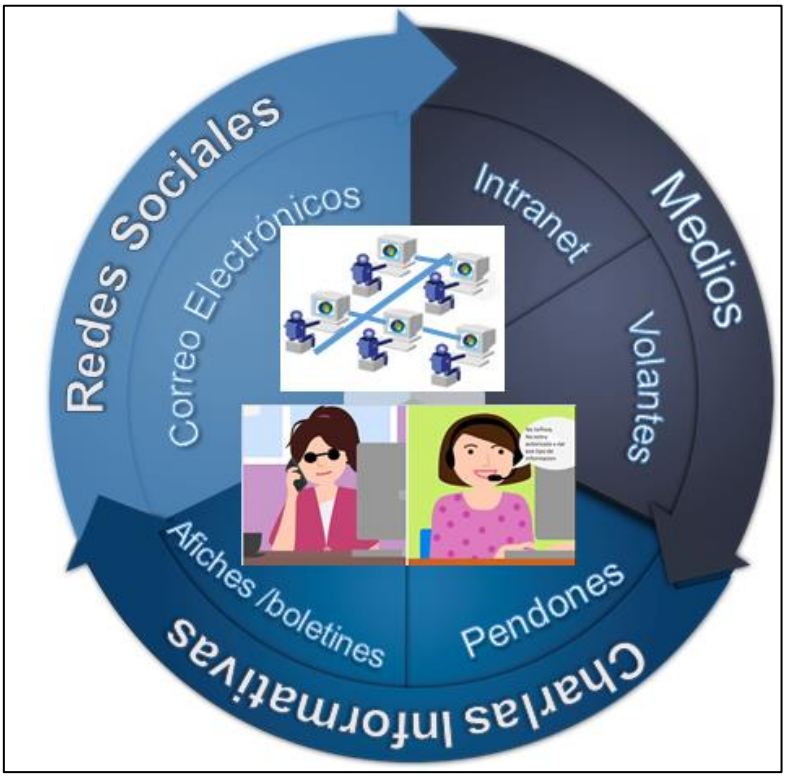

Figura 35 - Arquitectura de un esquema una vez el plan de sensibilización se ejecute (Fuente: Diseño Propio)

11. CONCLUSIONES

Mediante las actividades desarrolladas durante el presente proyecto se puede concluir lo siguiente:

- El ciberespacio es un ambiente donde se encuentra alojada o transita la mayor parte de la información que genera el ser humano en la actualidad; dicha información puede ser de tipo personal, pero también existe gran parte de la misma que es inherente a entidades y organizaciones de todo tipo, tanto público como privado. Los grandes volúmenes de información, disponible en el ciberespacio, y lo que la misma representa para las personas y organizaciones ha generado gran cantidad de amenazas que generan riesgos para la seguridad de personas e instituciones.

- Como cualquier tipo de amenaza, las cibernéticas han sido estudiadas y se han generado diferentes tipos de estrategias para hacer frente a las mismas; la mayor parte de estas estrategias han estado enfocadas en detectar incidentes y acciones maliciosas que se presenten dentro de las infraestructuras informáticas digitales de las diferentes entidades. El fundamento de estas estrategias ha sido principalmente el antiguo paradigma de la ciberseguridad, conocido como la "Defensa en Profundidad"; dicho paradigma busca fortalecer las medidas de seguridad perimetral asumiendo que la mayor parte de los factores de riesgo provienen del exterior del perímetro digital de cualquier tipo de organización; sin embargo, la inclusión de este paradigma dentro de las estrategias de ciberseguridad parece no haber permitido alcanzar los resultados esperados.

- De la mano de lo anterior se ha evidenciado un creciente esfuerzo que ha conducido al diseño y producción de todo tipo de tecnologías enfocadas hacia la detección de incidentes cibernéticos, lo que tampoco ha sido suficiente para disminuir la creciente presencia de incidentes cibernéticos dentro de las organizaciones, por lo que es importante asumir nuevas posturas de cara a la ciberseguridad.

- Muchas de las amenazas cibernéticas de la actualidad, se materializan exitosamente gracias a la influencia del factor humano en los sistemas informáticos digitales, por lo cual es indispensable que las organizaciones empiecen a diseñar programas de capacitación y entrenamiento que les brinden a los usuarios de los sistemas TIC las herramientas cognitivas que les permitan hacer frente a este tipo de amenazas de forma eficiente.

- Cualquier tipo de herramienta tecnológica orientada a la ciberseguridad de las organizaciones pierde su eficiencia si no es utilizada de forma correcta, por lo cual se requiere adelantar esfuerzos que les permitan a los usuarios de este tipo de sistemas ser conscientes de la importancia de su correcto uso.

12. BIBLIOGRAFÍA

[1] Consejo Nacional de Política Económica y Social República de Colombia, Departamento Nacional de Planeación, *Documento CONPES 3854*, Bogotá , Bogotá D.C., 2016.

[2] Infraestructura de Datos Espaciales de Perú, «GeoIDEP,» [En línea]. Available: http://www.geoidep.gob.pe/conoce-las-ides/metadatos/que-son-los-metadatos. [Último acceso: 29 marzo 2018].

[3] Qmee, «Blog Qmee,» 2015. [En línea]. Available: https://blog.qmee.com/online-in-60-seconds-infographic-a-year-later/. [Último acceso: 5 marzo 2018].

[4] N5 Computer Science, «Cybersecurity Fundamentals,» [En línea]. Available: http://cybersecurity.jhigh.co.uk/fundementals/growingCrime.html. [Último acceso: 2 marzo 2018].

[5] S. Bursztein, «Factor humano: el origen de los incidentes,» *Magazcitum. El magazine para los profesionales de la seguridad TI,* nº 3446, 2016.

[6] MVA Electrotécnia, «MVA Electrotécnia,» 2014. [En línea]. Available: http://www.mva.pt/info/noticias/1239. [Último acceso: 22 marzo 2018].

[7] Gemalto Security to be free, «Breach Level Index,» 2017. [En línea]. Available: http://breachlevelindex.com/. [Último acceso: 2 marzo 2018].

[8] Atrion, «Assumption of Breach a New Approach to Cyber Security,» 2016.

[9] R. Hernández Sampieri, C. Fernández Collado y M. d. P. Baptista Lucio, Metodología de la Investigación. Sexta Edición, México D.F.: McGRAW-HILL, 2014.

[10] EC-Council, Ethical Hacking and Countermeasures v9. Module 06: Malware Threats, EC-Council, 2015.

[11] J. D. Peláez, «INCIBE,» 26 noviembre 2013. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/metadatos-webs-empresas. [Último acceso: 25 marzo 2018].

[12] J. Wittkop, Building a comprehensive IT Security Program, Boulder, Colorado: Apress, 2016.

[13] S. Cobb, «We live Security by ESET,» 4 abril 2012. [En línea]. Available: https://www.welivesecurity.com/2012/04/04/byod-infographic-for-security-not-a-pretty-picture/. [Último acceso: 17 marzo 2018].

[14] E. Griffor, Handbook of system safety and security, Cambridge, MA: Syngress, 2017.

[15] J. V. Haaster, R. Gevers y M. Sprengers, Cyber Guerrilla, Cambridge, MA: Syngress, 2016.

[16] Mandiant Concsulting, M-TRENDS 2016 Asia Pacific Edition, FireEye Inc., 2016.

[17] M. Collins, Network Security Through Data Analysis, Sebastopol, CA: O'Reilly, 2014.

[18] K. K. Tarala y J. Tarala, Open Threat Taxonomy Ver 1.1., Venice, FL: Enclave Security, 2015.

[19] C. W. Lin y A. S. Vincentelli, Security - Aware Design for Cyber-Physical Systems, Cham: Sprienger, 2017.

13. REFERENCIAS

[1] Consejo Nacional de Política Económica y Social República de Colombia, Departamento Nacional de Planeación, *Documento CONPES 3854,* Bogotá , Bogotá D.C., 2016.

[2] Infraestructura de Datos Espaciales de Perú, «GeoIDEP,» [En línea]. Available: http://www.geoidep.gob.pe/conoce-las-ides/metadatos/que-son-los-metadatos. [Último acceso: 29 marzo 2018].

[3] Qmee, «Blog Qmee,» 2015. [En línea]. Available: https://blog.qmee.com/online-in-60-seconds-infographic-a-year-later/. [Último acceso: 5 marzo 2018].

[4] N5 Computer Science, «Cybersecurity Fundamentals,» [En línea]. Available: http://cybersecurity.jhigh.co.uk/fundementals/growingCrime.html. [Último acceso: 2 marzo 2018].

[5] S. Bursztein, «Factor humano: el origen de los incidentes,» *Magazcitum. El magazine para los profesionales de la seguridad TI,* nº 3446, 2016.

[6] MVA Electrotécnia, «MVA Electrotécnia,» 2014. [En línea]. Available: http://www.mva.pt/info/noticias/1239. [Último acceso: 22 marzo 2018].

[7] Gemalto Security to be free, «Breach Level Index,» 2017. [En línea]. Available: http://breachlevelindex.com/. [Último acceso: 2 marzo 2018].

[8] Atrion, «Assumption of Breach a New Approach to Cyber Security,» 2016.